MASTER'S THESIS

Het ontwerp van een GDPR maturity model op basis van enterprise architectuur en datamanagement

Hess, T.G. (Thijs)

Award date:
2019

Het ontwerp van een GDPR maturity model op basis van enterprise architectuur en datamanagement

The design of a GDPR Maturity Model based on Enterprise Architecture and Data Management

Opleiding:	Open Universiteit, faculteit Management, Science & Technology Masteropleiding Business Process Management & IT
Programme:	Open University of the Netherlands, faculty of Management, Science & Technology Master Business Process Management & IT
Cursus:	IM9806 Afstuderen BPMIT
Student:	Thijs Hess
Identiteitsnummer:	
Datum:	21/08/2019
Afstudeerbegeleider	Ben Roelens
Meelezer	Laury Bollen
Versie nummer:	2.0
Status:	Definitief

Abstract

Vanaf 25 mei 2018 is de General Data Protection Regulation (GDPR) van toepassing in alle lidstaten van de Europese Unie. Hoewel organisaties moeten kunnen aantonen dat zij aan de GDPR voldoen, zijn er momenteel geen meetinstrumenten beschikbaar om de *maturity* (volwassenheid) van een organisatie op het gebied van de GDPR objectief te meten. In dit onderzoek is daarom een GDPR *maturity model* ontwikkeld op basis van bestaande modellen binnen enterprise architectuur (EA) en datamanagement (DM) om de *maturity* op het gebied van de GDPR te meten. Qua EA is gebruikgemaakt van het GOA 2.0 en OMB EA 3.1, qua DM is gebruikgemaakt van de MD3M, DCAM en DMM-modellen. Het *maturity model* is in de praktijk toegepast en daarna inhoudelijk en praktisch geëvalueerd op basis van de input van vier experts bij twee grote publieke organisaties, met respectievelijk 3.000 en 58.000 medewerkers. Het *maturity model* maakt het mogelijk om de mate waarin wordt voldaan aan de GDPR vast te stellen op basis van gestructureerde interviews. Hierbij worden er aspecten uit EA en DM meegewogen waardoor het model een bredere inkijk biedt dan sec de GDPR. Het GDPR *maturity model* maakt het mogelijk om de *maturity*, de mate waarin wordt voldaan aan de GDPR, vast te stellen op basis van gestructureerde interviews.

Sleutelbegrippen

Nederlands: General Data Protection Regulation, maturity model, Enterprise Architecture, Data Management, Design Science Research

Samenvatting

Vanaf 25 mei 2018 is de General Data Protection Regulation (GDPR) van toepassing in alle lidstaten van de Europese Unie. De wetgeving is van toepassing op een groot deel van de organisaties die binnen de Europese Unie persoonsgegevens verwerken. De verantwoordingsplicht voor een voldoende toepassing van de GDPR ligt bij de organisaties zelf. Het vellen van een eigen oordeel door de organisaties geeft een subjectief beeld over de implementatie van de GDPR binnen een organisatie. Hoewel organisaties moeten kunnen aantonen dat zij aan de GDPR voldoen, zijn er momenteel geen meetinstrumenten beschikbaar om de *maturity* van een organisatie op het gebied van de GDPR objectief te meten. In dit onderzoek is daarom een *maturity model* ontwikkeld op basis van bestaande modellen binnen enterprise architectuur (EA) en datamanagement (DM) om de *maturity* op het gebied van de GDPR te meten. Om de validiteit en betrouwbaarheid van dit onderzoek te waarborgen, zijn de principes van Design Science Research Methodology toegepast.

Het ontwikkelde *maturity model* is gebaseerd op bestaande *maturity models* uit EA en DM. Voor EA is gebruikgemaakt van het GOA 2.0 en OMB EA 3.1, voor DM is gebruikgemaakt van de MD3M, DCAM en DMM-modellen. Deze modellen zijn de basis geweest voor de vorming van het *maturity model* voor de GDPR, waaruit relevante criteria en *maturity levels* zijn afgeleid. Voor de GDPR zijn de kernaspecten integriteit en vertrouwelijkheid, opslagbeperking, juistheid, rechtmatigheid, behoorlijkheid en transparantie als uitganspunt genomen. Het *maturity model* kent zes *maturity*-niveaus van nul tot en met vijf en is meetbaar gemaakt door middel van een vragenlijst. Het model is in de praktijk toegepast en daarna verbeterd op basis van de input van experts bij twee grote publieke organisaties, met respectievelijk 3.000 en 58.000 medewerkers.

De eerste iteratie van het model heeft geleid tot het aanpassen van 9 en het schrappen van 1 van de 35 vragen in de vragenlijst en tot het aanpassen van 4 deelgebieden binnen de categorie juistheid. De eerste iteratie had een algemene tevredenheidsscore van 7 uit 10. Op basis van de input uit de interviews zijn de 9 vragen aangepast en opnieuw voorgelegd aan de experts, samen met de algemene scoring. Na het aanpassen van het GDPR *maturity model* en de bijbehorende interviewvragen, zijn de aangepaste vragen opnieuw middels een vragenlijst uitgezet bij de vier experts. Dit heeft bij 4 van de 9 aangepaste vragen geresulteerd in een algemene consensus, bij 4 vragen tot consensus op basis van stabiliteit en bij 1 vraag tot een gebrek aan consensus. De algemene tevredenheidsscore is daarnaast met een halve punt toegenomen tot een 7,5.

Het GDPR *maturity model* maakt het mogelijk om de *maturity*, de mate waarin wordt voldaan aan de GDPR, vast te stellen op basis van gestructureerde interviews.

Summary

The General Data Protection Regulation (GDPR) has been in effect in all member states of the European Union since May 25, 2018. The legislation applies to a large proportion of the organizations that process personal data within the European Union. Accountability for sufficient application of the GDPR lies with the organizations processing the data. Self-assessment conducted by the organizations provides a subjective picture of GDPR implementation within the organizations. Although organizations must be able to demonstrate that they comply with the GDPR, there are currently no instruments that objectively measure the maturity of an organization's application of the GDPR. In the study described in this paper, a maturity model based on existing models enterprise architecture (EA) and datamanagement (DM) was developed and validated to measure maturity in the field of the GDPR. To guarantee the validity and reliability of this study, the principles of design science research methodology were applied.

The maturity model is based on existing maturity models from EA and DM. For EA, the GOA 2.0 and OMB EA 3.1 were used, and for DM, the MD3M, DCAM, and DMM models were used. Relevant criteria and maturity levels were derived from the existing models. The key aspects of the GDPR are integrity and confidentiality, storage limitation, accuracy, lawfulness, fairness and transparency, purpose limitation, and data minimization. The model has six maturity levels ranging from zero to five that are measured using a questionnaire. The model was implemented and later improved based on the input of experts from two large public organizations, with 3,000 and 58,000 employees.

The first iteration of the model led to the adjustment of nine and the removal of one of the 35 questions in the questionnaire, the adjustment of four maturity cells at the level of accuracy, and an overall satisfaction score of seven out of ten. Based on the input from the interviews, the nine questions were adjusted and resubmitted to the expert along with the general scoring for the overall model. After adjusting the GDPR maturity model and the accompanying interview questions, the adjusted questions were again submitted to the four experts. This resulted in consensus based on stability for four of the nine adapted questions. There was no consensus for one of the questions. The overall satisfaction score also increased by half a point to seven and a half out of ten.

The GDPR maturity mode makes it possible to determine the maturity and degree of compliance with the GDPR based on structured interviews. Aspects from EA and DM are considered so that the model offers a broader perspective than the GDPR. The maturity levels are derived from existing models.

Inhoudsopgave

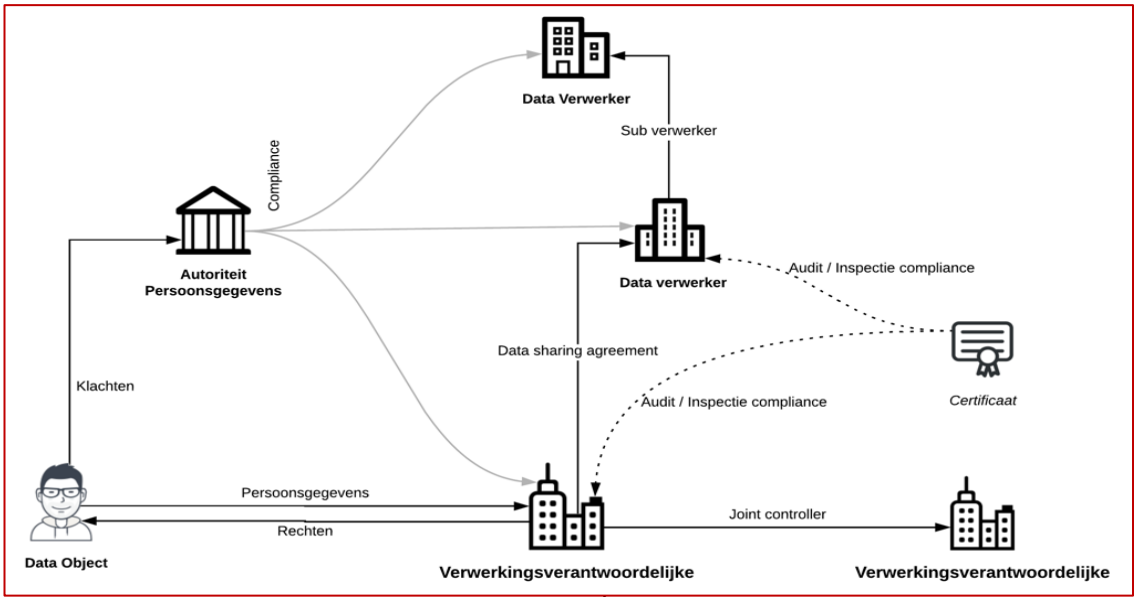
1. Introductie

1.1. Achtergrond

Vanaf 25 mei 2018 is de General Data Protection Regulation (GDPR) van toepassing in alle lidstaten van de Europese Unie. De wetgeving is van toepassing op een groot deel van de organisaties die binnen de Europese Unie persoonsgegevens verwerken. De uitvoeringswet Algemene Verordening Gegevensbescherming (AVG) is de specifieke regelgeving die van toepassing is binnen Nederland (Schermer, Hagenauw, & Falot, 2018). De AVG is niet van toepassing op de verwerking van persoonsgegevens in het kader van opsporing en berechting of activiteiten die buiten het unierecht vallen, zoals verwerking op basis van de Wet op de inlichtingen- en veiligheidsdiensten. Sancties voor de overtreding van de bepalingen over de principes, rechtsgrondslagen en rechten van betrokkenen kunnen worden gesanctioneerd met een administratieve boete van maximaal 20 miljoen euro of 4% van de jaaromzet.

De GDPR geeft personen meer rechten over hun eigen gegevens. Zo krijgen personen het recht eigen gegevens in te zien en deze te laten verwijderen. Deze GDPR heeft verregaande implicaties voor de wijze waarop organisaties persoonsgegevens mogen verwerken, registeren en opslaan.

De GDPR maakt duidelijk onderscheid in de rechten en plichten van de bij de verwerking van persoonsgegevens betrokken partijen. (Schermer et al., 2018) (zie figuur 1). De verwerkingsverantwoordelijke is degene die 'doel en middelen' bepaalt voor de verwerking, degene die met andere woorden bepaalt hoe en waarom persoonsgegevens worden verwerkt. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van de GDRP-beginselen en moet te allen tijde kunnen aantonen dat de verwerking van de persoonsgegevens aan de GDPR voldoet. De dataverwerker verwerkt de gegevens van personen voor een bepaald doel en handelt in opdracht van de verwerkingsverantwoordelijke. De verantwoordelijkheid voor de verwerking kan voortvloeien uit een juridische bevoegdheid, een impliciete bevoegdheid (bijvoorbeeld gegevens van werknemers verwerken), een feitelijke invloed of een gezamenlijke verantwoordelijkheid. Iedere Europese lidstaat moet een toezichthouder aanstellen om te controleren of de verwerkingsverantwoordelijke en dataverwerker zich aan de vastgelegde regels en verplichtingen uit de GDPR houden, in Nederland is dat de Autoriteit Persoonsgegevens (AP).



Figuur 1. Relaties tussen de verschillende rollen binnen de Nederlandse AVG uitvoeringswet. Gebaseerd op Pandit, O'Sullivan en Lewis (2018).

1.2. Gebiedsverkenning

De implementatie van de GDPR vereist grote veranderingen met betrekking tot de interne datastructuur van een organisatie. Twee onderzoeksgebieden die nagaan hoe data efficiënt gebruikt kunnen worden in een organisatie zijn *enterprise* architectuur (EA) en datamanagement (DM).

EA is het onderzoeksgebied dat processen, structuren, applicaties en systemen geïntegreerd probeert te beschrijven (Lankhorst, 2009). EA-raamwerken zijn een coherent geheel van principes, methodes en modellen om een geïntegreerd beeld te geven van de strategie, structuur, processen, informatiesystemen en technologie van een onderneming (Lankhorst, 2009, p. 3). Binnen EA worden verschillende methodes en technieken gebruikt om een architectuur vorm te geven. Een voorbeeld van een EA-framework is The Open Group Architecture Framework (The open group, 2018) . De TOGAF volgt vijf principes, te weten: begrijpbaar, robuust, compleet, consistent en stabiel, zoals weergegeven in Bijlage 1.

DM beschrijft de processen die gebruikt worden om data te plannen, te specificeren, te creëren, te verwerven, te onderhouden, te gebruiken, te archiveren, op te halen, te controleren en te corrigeren (DAMA, 2014). Het doel van DM is compliance, het faciliteren van besluitvorming en vergroting van de efficiëntie en effectiviteit om integratie van bedrijfsonderdelen te ondersteunen (Brous, Janssen, & Vilminko-Heikkinen, 2011).

Hoewel de termen data en informatie vaak door elkaar gebruikt worden, zijn ze wezenlijk verschillend. Zo zijn data een set van karakters die zonder context geen betekenis hebben (Brous et al., 2011), terwijl informatie data is die in context is geplaatst of is verwerkt. DM is gebaseerd op de vier principes (Organisatie, *Alignment*, *Compliance, Common understanding*) weergegeven in Bijlage 2 (Brous et al., 2011). Een bekend raamwerk is DAMA-DMBOK, dat een verzameling vormt van processen, kennisgebieden en best practices binnen DM (DAMA, 2014). Het DAMA-DMBOK kent de volgende kennisgebieden: data governance, data architecture, data modeling en design, data storage en operations, data security, data integration en interoperability, document en content, reference en master data, data warehousing en BI, metadata en data quality.

1.3. Probleemstelling

De verantwoordingsplicht voor een voldoende toepassing van de GDPR ligt bij de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke kan maatregelen vastleggen in bijvoorbeeld gegevensbeschermingsbeleid. Beoordeling van de implementatie van de GDPR door de verwerkingsverantwoordelijke zelf geeft een subjectief beeld. Er zijn momenteel echter nog geen instrumenten beschikbaar binnen de wetenschappelijke literatuur om de mate van implementatie van de GDPR binnen een organisatie objectief vast te stellen. EA en DM bieden een wetenschappelijke basis om dit probleem op te lossen doordat zij beschikken over *maturity models*.

De probleemstelling luidt als volgt:

Hoewel organisaties moeten kunnen aantonen dat zij aan de GDPR voldoen, zijn er momenteel geen meetinstrumenten beschikbaar om de *maturity* van een organisatie op het gebied van de GDPR objectief te meten.

1.4. Opdrachtformulering

Maturity models zijn een belangrijk instrument binnen EA en DM omdat zij de huidige stand van een organisatie weer te geven en opties voor verbetering inzichtelijk maken (Becker, Knackstedt, & Poppelbus, 2009). Met het gebruik van *maturity models* worden kernaspecten getoetst aan de verschillende *maturity levels* om zo een beeld te krijgen van de mate waarin een organisatie effectief EA en DM toepast. Resultaten van een dergelijke evaluatie bieden een richtsnoer voor het verbeteren van de toepassing van EA en DM (Aiken, 2007).

Het aantonen van GDPR compliance op een objectieve manier kan ondersteund worden door de ontwikkeling van een overeenkomstig *maturity model*. Voor de GDPR is een dergelijk instrument momenteel echter niet beschikbaar. In dit onderzoek wordt daarom een *maturity model* ontwikkeld op basis van bestaande modellen binnen EA en DM om de *maturity* op het gebied van de GDPR te meten.

De onderzoeksvraag luidt aldus als volgt:

> *Hoe kan het maturity-niveau van een organisatie op het gebied van de GDPR worden gemeten, zodat het management en externe actoren in staat zijn om de mate van compliance objectief vast te stellen?*

De onderzoeksvraag valt uiteen in vijf deelvragen:

1. Welke *maturity models* binnen EA en DM kunnen de basis vormen voor een GDPR *maturity model*?
2. Welke kernaspecten van GDPR-*maturity* kunnen worden afgeleid uit *maturity models* binnen EA en DM?
3. Welke *maturity levels* voor GDPR-*maturity* kunnen worden afgeleid uit *maturity models* binnen EA en DM?
4. Welke criteria zijn nodig voor het beschrijven van de *maturity*-niveaus van de GDPR-aspecten?
5. Hoe kan het *maturity model* in de praktijk worden gevalideerd?

Om de kwaliteit en betrouwbaarheid van dit onderzoek te waarborgen, zullen de principes van Design Science Research Methodology worden toegepast (Hevner, March, Park, & Ram, 2004). Deze methodologie is in het bijzonder geschikt omdat het onderzoek zowel gericht is op het ontwerp als de validatie van het *GDPR maturity model*, wat gezien kan worden als een IS (*information systems*)-artefact. In dit onderzoek worden twee 'Design Science artefacten' ontwikkeld: het te ontwikkelen *maturity model* (i.e., een model) en het toegepaste model in de organisatie (i.e., een instantie). Daartoe wordt globaal het stappenplan van Peffers et al. (2008) gebruikt, dat uit zes stappen bestaat, te weten: (i) problem identification en motivation, (ii) definition of solution objectives, (iii) design en development, (iv) demonstration, (v) evaluation, en (vi) communication.

1.5. Motivatie en relevantie

Organisaties verwerken steeds vaker en steeds meer persoonsgegevens. De bescherming van die persoonsgegevens is een grondrecht van burgers. De ontwikkeling van een *maturity model* voor de GDPR is niet alleen van belang voor personen van wie gegevens worden verwerkt, maar ook voor de organisaties die persoonsgegevens verwerken. Een *maturity model* biedt immers inzicht in de mate

van GDPR *maturity* en in mogelijke aandachtsgebieden voor verbetering. Het niet kunnen voldoen aan de GDPR kan ontwrichtend werken voor een organisatie en tot reputatieschade en sancties leiden. Boetes kunnen oplopen tot 20 miljoen euro of 4% van de wereldwijde jaaromzet (Schermer et al., 2018, p. 91). Het is daarom maatschappelijk relevant dat een objectief GDPR *maturity model* ontwikkeld wordt, zowel om bedrijven te helpen bij het naleven van de GDPR als om gegevens van natuurlijke personen te beschermen. De relevantie van dit onderzoek wordt hieronder verder besproken vanuit een drietal perspectieven, te weten: GDPR, EA, en DM.

GDPR

De GDPR biedt zelf geen handvatten voor het meten van de mate waarin organisaties voldoen aan de GDPR. Organisaties kunnen zelf risicoanalyses uitvoeren, zoals *Privacy Impact Assessments* (PWC Nederland, 2017). Een *Privacy Impact Assessment* (PIA) is echter gericht op applicaties en niet op de organisatie als geheel. Een *maturity model* biedt daarom een meer omvattende kijk. In 2018 heeft de Digitale Overheid het *Privacy Maturity Model* ontwikkeld: "Deze tool vormt een meetlat, waarlangs de *maturity* van de organisatie gemeten kan worden in de mate waarin privacybescherming in de organisatie is afgedekt" (Digitale overheid, 2017). Het *Privacy Maturity Model* is dus voornamelijk gericht op privacybescherming en niet op de implementatie van de GDPR als geheel.

EA

De GDPR heeft impact op EA en maakt een *data lifecycle*-benadering binnen EA noodzakelijk (Henderson, 2018). ICT-instrumenten kunnen hieraan bijdragen door verzoeken van klanten over de gebruikte data te monitoren, inbreuken te detecteren en gegevens te anonimiseren. Een *maturity model* maakt de resultaten van de verschillende inspanningen om tot verbeteringen te komen meetbaar. De ontwikkeling van EA *maturity models* kent een lange geschiedenis, maar deze *models* zijn vaak conceptueel, waardoor de relevantie beperkt blijft. Onderwerpgerichte modellen kunnen de relevantie van een model vergroten en de kwaliteit verbeteren. Het is hierbij raadzaam om bestaande modellen te onderzoeken voor het ontwikkelen van nieuwe modellen (Wendler, 2012).

DM

Met de komst van de GDPR is een toenemend belang van transparantie en het afleggen van verantwoording op het gebied van DM ontstaan. Een *maturity model* kan een bijdrage leveren aan deze verantwoording. Tikkinen-Piri, Rohunen en Markkula (2018) stellen dat met de komst van de GDPR het voor bedrijven van toenemend belang is om aan te tonen dat zij voldoende maatregelen hebben genomen op het gebied van (onder andere) DM. Door aan te tonen dat organisaties voldoen aan de GDPR kan het vertrouwen in organisaties toenemen. Freiherr en Zeiter (2018) stellen dat er in de toekomst meer transparantie op het gebied van DM zal worden geëist, waardoor de wijze waarop data wordt verwerkt uitgebreider zal moeten worden vastgelegd dan in het verleden het geval was.

1.6. Aanpak in hoofdlijnen

Het onderzoek wordt in stappen uitgevoerd. In hoofdstuk 1 wordt de inleiding en probleemstelling beschreven. In hoofdstuk 2 wordt het ontwerp van het onderzoek uiteengezet, waarvoor gebruik is gemaakt van de Design Science Research-methode als overkoepelende methodologie voor dit onderzoek. In hoofdstuk 3 komen de resultaten van de literatuurstudie aan bod. Hierbij wordt alle theoretische kennis die noodzakelijk is bij de ontwikkeling van een GDPR *maturity model* in kaart gebracht. De literatuurstudie geeft antwoord op de eerste vier deelvragen. De uitvoering van het empirisch onderzoek van het model wordt behandeld in hoofdstuk 4. Voor de ontwikkeling van het

model zijn twee interactieve cycli uitgevoerd. In hoofdstuk 5 komen tot slot de aanbevelingen, de conclusie en de reflectie op het onderzoek aan de orde.

De eerste twee stappen worden uitgevoerd in de literatuurfase (VAF) en de laatste stap in de empirische fase (AF). De activiteiten in de verschillende stappen worden gestuurd door de probleemstelling uit paragraaf 1.3, waarbij van belang is dat deze probleemstelling wordt aangescherpt met inzichten uit de literatuurfase.

2. Methodologie

Dit hoofdstuk beschrijft de opzet van deze studie. Het ontwerp van de studie is gekoppeld aan verschillende methoden en technieken.

2.1. Conceptueel ontwerp: keuze van onderzoeksmethode(n)

Sinds de invoering van de GDPR in alle EU-lidstaten moeten organisaties kunnen aantonen dat zij aan de GDPR voldoen. Er zijn momenteel echter geen objectieve meetinstrumenten beschikbaar om dit te meten.

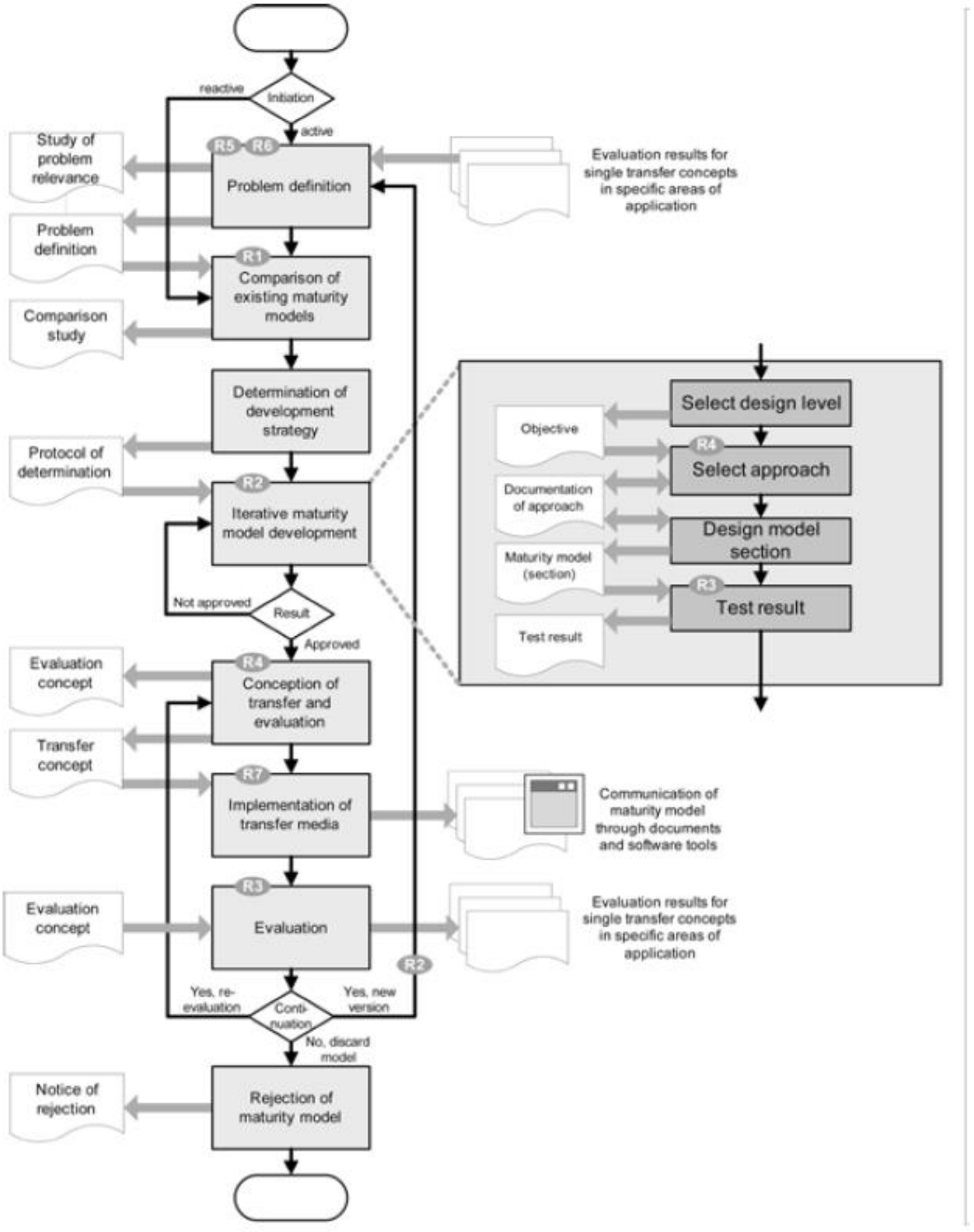
De ontwikkeling van een GDPR *maturity model* maakt het mogelijk om de implementatie van de wetgeving door de organisatie op een objectieve manier te kunnen vaststellen.

Het GDPR *maturity model* is ontwikkeld met gebruikmaking van de Design Science Research-methode (Hevner et al., 2004; Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007). Het ontwerp van het model is gebaseerd op relevante EA & DM *maturity models*. Validatie van het GDPR-model vond vervolgens plaats in een praktijksituatie. De Design Science Research-methode is een overkoepelende methode waarbinnen aanvullende methodes gebruikt kunnen worden voor het ontwerp en of de evaluatie van artefacten. Aan de basis van de Design Science-methodologie ligt een cyclus van 'bouwen' en 'evalueren' en vier artefacten, te weten: constructen, modellen, methoden en instanties (Hevner et al., 2004). In dit onderzoek komen twee van deze artefacten aan bod, het GDPR *maturity model* (i.e., een model) en een instantie (i.e., het toegepaste GDPR *maturity model* in een praktijkcontext).

De methode is gebaseerd op zes processtappen, te weten: probleemidentificatie en -motivatie, het definiëren van een oplossing, ontwerp en ontwikkeling, demonstratie, evaluatie en communicatie. In hoofdstuk 1 (paragraaf 1.3) is de probleemidentificatie en motivatie beschreven en is een hoofdoplossingsrichting gedefinieerd. De oplossing (artefact) betreft een GDPR *maturity model* om een objectieve meting van GDPR *maturity* mogelijk te maken. In paragraaf 1.4 is deze oplossing verder gedefinieerd. Om het GDPR *maturity model* te ontwerpen, zijn in hoofdstuk 3 *maturity models* uit de gerelateerde disciplines EA en DM onderzocht. Uit deze modellen zijn de relevante aspecten, criteria en *maturity levels* afgeleid die de basis vormen voor het GDPR *maturity model*. In hoofdstuk 4 wordt dit model gedemonstreerd en geëvalueerd bij twee grote organisaties, waarin de GDPR van toepassing is (dat wil zeggen: één ontwerpcyclus met twee organisaties). Middels de publicatie van deze scriptie binnen de Open Universiteit worden de resultaten gecommuniceerd en zijn deze vrij toegankelijk voor publiek.

2.2. Technisch ontwerp: uitwerking van de methode

Als overkoepelende methodologie voor dit onderzoek is gebruikgemaakt van de Design Science Research-methode. Voor de ontwikkeling van het *maturity model* is meer specifiek het model van Becker et al. (2009) gebruikt. Figuur 2 beschrijft het proces voor de ontwikkeling van het *maturity model*. Becker et al. (2009) beschrijven zeven stappen voor de ontwikkeling van een *maturity model,* te weten: het formuleren van de probleemdefinitie, de vergelijking met bestaande modellen, het bepalen van de ontwikkelstrategie, iteratief ontwikkelproces, ontwerp voor overdracht en evaluatie, implementatie en overdracht en tot slot evaluatie. Deze stappen worden hieronder op dit onderzoek betrokken.



Figuur 2. Procedure voor ontwikkeling maturity models (Becker et al., 2009, p. 218)

Probleemdefinitie

Organisaties verwerken steeds vaker en steeds meer persoonsgegevens. De bescherming van persoonsgegevens is een grondrecht, dat bescherming moet bieden aan de betrokkene om wiens persoonsgegevens het gaat. De ontwikkeling van een *maturity model* voor de GDPR is niet alleen van belang voor personen van wie gegevens worden verwerkt, maar ook voor de organisaties die

persoonsgegevens verwerken. Een *maturity model* biedt immers inzicht in de mate van GDPR *maturity* en in mogelijke aandachtsgebieden voor verbetering.

Vergelijking met bestaande modellen

Het ontwikkelde *maturity model* is gebaseerd op bestaande *maturity models* uit EA en DM. In hoofdstuk 3 is de opbouw van de literatuurstudie beschreven en is gezocht naar relevante *maturity models* voor EA en DM. De gevonden modellen zijn getoetst op een aantal vaststaande criteria, te weten: gebruik van de Engelse taal, de inhoudelijke relatie met EA of DM en de volledige beschikbaarheid van de tekst.

Voor EA is gebruikgemaakt van het GOA 2.0 (United States Government Accountability Office, 2012) en OMB EA 3.1 (The Office of Management and Budget, 2009), voor DM zijn de MD3M (Spruit & Pietzka, 2014), DCAM (CMMI Institute, 2018) en DMM (DAMA, 2014) modellen gehanteerd. Deze modellen lagen aan de basis van het GDPR *maturity model*; relevante criteria en *maturity levels* zijn uit deze modellen afgeleid.

Bepalen van de ontwikkelstrategie

Binnen zowel EA als DM zijn bestaande m*aturity models* die de huidige stand van een organisatie binnen EA en DM weergeven en opties voor verbetering inzichtelijk maken (Becker et al., 2009). In *maturity models* worden kernaspecten getoetst aan verschillende *maturity levels.* Voor de ontwikkeling van het GDPR *maturity model* zijn de kernaspecten van de bestaande *maturity models* geïnventariseerd en waar mogelijk vertaald naar een GDPR *maturity model.* Hiervoor zijn verschillende criteria uit de bestaande modellen gekoppeld aan de hand van de kernaspecten binnen GDPR (zie paragraaf 3.3.1) en vervolgens geïntegreerd om te komen tot relevante GDPR-criteria (zie Bijlage 14). Het aantonen van GDPR compliance op een objectieve manier is ten slotte ondersteund door de ontwikkeling van het *maturity model* (zie paragraaf 3.5).

Iteratief proces

In deze studie zijn twee interactieve cycli uitgevoerd voor de ontwikkeling van het *maturity model*. Na samenstelling is het model in twee cycli bij twee organisaties geëvalueerd. Vanwege de beperkte tijd die voor dit onderzoek staat is gekozen voor slechts twee cycli.

Ontwerp voor transfer en evaluatie

Het m*aturity model* is in de praktijk getoetst door het afnemen van de *technology acceptance model* (TAM) vragenlijst (Davis, 1989). Er is getoetst op basis van de intentie voor gebruik, de bruikbaarheid en het gebruiksgemak. Middels de Delphi-studie (De Bruin, 2007) zijn de vragen van het model inhoudelijk geëvalueerd. Het GDPR *maturity*-niveau is eerst vastgesteld door het afnemen van een gestructureerde vragenlijst. Na het vaststellen van het *maturity* model zijn de vragen van het model voorgelegd aan vier experts op het gebied van de GDPR middels een vragenlijst. Middels deze vragenlijst worden de vragen van het model beoordeeld op basis van relevantie, uitgedrukt in een zevenpunts-Likertschaal. Ook zijn de experts gevraagd naar de verwachte bruikbaarheid en het gebruiksgemak door gebruik te maken van de TAM-vragenlijst (Davis, 1989). Daarnaast is een algemene tevredenheidsscore gegeven. De input (TAM scoring en de scoring van de vragen) van de experts vormde de basis voor het tweede semigestructureerde interview waarbij twee experts (één per organisatie) zijn gevraagd naar verbetermogelijkheden voor het model. Op basis van de scoring en de interviews zijn wijzigingen in de vragenlijst en het model aangebracht.

Implementatie en overdracht

Middels demonstratie van het GDPR *maturity model* binnen twee organisaties wordt het model in hoofdstuk 4 in de praktijk geïmplementeerd.

Evaluatie

In hoofdstuk 4 zijn de resultaten en aanpassingen van het model naar aanleiding van de voorgaande processtappen weergegeven.

2.3. Gegevensanalyse

In de demonstratie- en evaluatiefase van deze studie is de casestudybenadering van Yin (2003) gebruikt. Hierbij is deelvraag 5 'Hoe kan het *maturity model* in de praktijk worden gevalideerd?' beantwoord. Doel is het ontwikkelde GDPR m*aturity model* te valideren door toepassing in de praktijk, om zo verbeteringen in het ontwerp te identificeren. Volgens Yin is een casestudy "een empirisch onderzoek dat een hedendaags fenomeen bestudeert binnen zijn context in de praktijk" (Yin, 2003, p. 13). Yin beschrijft verschillende wijzen waarop een casestudy kan worden vormgegeven. Er is gebruikgemaakt van een multipele casestudy om het ontwikkelde *maturity* model te testen. Het model is concreet in twee organisaties toegepast en geëvalueerd.

Om de geschiktheid van het ontwikkelde model te onderzoeken is gebruikgemaakt van het TAM (Davis, 1989). Het TAM gaat uit van het verband tussen de verwachte bruikbaarheid (*perceived usefulness*, PU) en het verwachte gebruiksgemak (*perceived ease of use*, PEOU) van de toepassing, wat nodig is om de bereidheid voor het gebruik van de toepassing (*intention to use*, IU) te kunnen voorspellen. In Bijlage 18 is de gehanteerde vragenlijst weergegeven. Het betreft een vertaling uit het Engels waarbij de vragen zijn geherformuleerd voor het GDPR m*aturity model*. De TAM-enquête is afgenomen bij vier experts binnen de twee onderzochte organisaties. De zestien vragen zijn uitgedrukt in de zevenpunts-Likertschaal van zeer oneens tot zeer eens.

Tevens zijn de afgeleide vragen uit het *maturity model* voorgelegd aan de experts. Hierbij is de mate waarin de vragen relevant zijn om een GDPR-aspect te beschrijven bevraagd, dit is tevens gedaan op de zevenpunts- Likertschaal, variërend van zeer oneens (1) tot zeer eens (7). Vragen waarbij geen sprake was van consensus of stabiliteit zijn gewijzigd of geschrapt. Voor consensus moest 50% van de respondenten het minstens eens (6-7) of oneens (1-2) zijn met de relevantie van een vraag om de GDPR-volwassenheid te beschrijven. Daarnaast moest 75% van de respondenten het minstens enigszins eens (5-6-7) of oneens (1-2-3) zijn en mocht er geen sprake zijn van tegenstrijdige scores. Verder moest het interkwartielbereik anderhalve punt of lager zijn (Van Looy, De Backer, Poels, & Snoeck, 2013). Als geen sprake was van consensus, is gebruikgemaakt van het stabiliteitscriterium volgens Randolph's (2005) free-marginal multirater kappa, waarbij de score groter of gelijk aan 0.4 moet zijn om een vraag definitief te kunnen aanvaarden. Tot slot is gevraagd een algemene tevredenheidsscore te geven over het ontworpen model op een elfpuntsschaal van 0 (laagst) tot en met 10 (hoogst).

Vanwege de beperkte omvang van het onderzoek was het onmogelijk om statistische testen uit te voeren op de resultaten van de multiple casestudy in de twee organisaties. Om een beter inzicht te krijgen zijn semigestructureerde interviews afgenomen waarbij is gevraagd naar de redenen achter het toekennen van de opgegeven scores.

2.4. Reflectie ten aanzien van validiteit, betrouwbaarheid en ethische aspecten

2.4.1. Betrouwbaarheid en validiteit

Yin (2003) beschrijft vier kwaliteitsvormen voor een casestudy ontwerp: constructvaliditeit, interne validiteit, externe validiteit en betrouwbaarheid. Deze worden hieronder uitgelegd.

Constructvaliditeit

Constructvaliditeit is de mate waarin de oplossing aan de doelstelling voldoet en meet wat gemeten moet worden. Om de constructvaliditeit te waarborgen is gebruikgemaakt van de bestaande kwantitatieve evaluatiemethode: het TAM van Davis (1989). Het TAM is een beproefd model in verschillende contexten met verschillende schalen. Hendrickson, Massey en Cronan(1993) hebben daarbij een hoge betrouwbaarheid aangetoond. Szajna (1994) heeft aangetoond dat het TAM toepasbaar is om de bereidheid tot het gebruik (i.e. *intention to use*), het zelfgebruik en de gebruiksattitude van een toepassing te meten. Deze onderzoeken hebben de geldigheid van het TAM bevestigd door gebruik van verschillende populaties van gebruikers en voor verschillende softwarekeuzes.

Om te toetsen of consensus over de vragen bestaat, is gebruikgemaakt van de methode Van Looy (Van Looy et al., 2013). Middels het afnemen van een vragenlijst, afgewisseld met gecontroleerde feedback, is de meest betrouwbare consensus van een expertpanel bereikt. Er is gebruikgemaakt van twee rondes middels een Delphi-studie, omdat de iteratieve aanpak de validiteit ten opzichte van een enkele ronde verbetert. De methode van Van Looy heeft in het verleden zijn nut bewezen om de relevantie van de inhoud van bestaande *business process maturity models* (BPMM) te evalueren. De oplossingsconstructie en -methodologie zijn transparant, zijn gegrond in de literatuur, zijn ontwikkeld met een iteratief oplossingsproces en bieden inzicht in beslissingscriteria en -afwegingen.

Interne validiteit

Om de interne validiteit van het onderzoek te waarborgen, zijn maatregelen genomen om verstorende (derde) factoren zo veel mogelijk uit te sluiten. Zo zijn vergelijkbare omstandigheden, zoals de bestede tijd per organisatie, gebruikt bij het toepassen en evalueren van het *maturity model*. Het onderzoek leent zich niet voor statistische testen; de evaluatie van het model is daarom ondersteund door semigestructureerde interviews, ofwel *'expert opinions'*. Binnen de twee organisaties zijn bij personen met veel kennis van de GDPR en de betreffende organisatie twee interviews afgenomen: één interview om het model toe te passen en één interview om het model te evalueren. De personen dienden hierbij zowel over kennis van het IT-landschap als over kennis van de implementatie van de GDPR binnen de organisatie te beschikken.

Externe validiteit

Ter vergroting van de externe validiteit is gebruikgemaakt van twee verschillende organisaties. Daarnaast komt de externe validiteit voort uit analytische generalisatie door replicatie van het onderzoek bij een ander type organisatie. Het gebruik van de verschillende modellen (EA en DM) als basis voor het *maturity model* draagt ook bij aan de externe validiteit. De basis van het nieuwgevormde *maturity model* is gelegen in generieke *maturity models* die hun werkzaamheid binnen diverse organisaties hebben bewezen. Om de externe validiteit verder te vergroten, zouden

additionele cases moeten worden onderzocht, maar dit was binnen het tijdsbestek door voor dit onderzoek stond onmogelijk.

Betrouwbaarheid
Betrouwbaarheid is de mate waarin een meting vrij is van willekeurige meetfouten (Saunders, 2015). Met andere woorden: een onderzoek is betrouwbaar als dezelfde resultaten oplevert bij herhaling. De betrouwbaarheid van dit onderzoek wordt gegarandeerd door de data (de scoring van de vragenlijsten) als bijlage aan deze scriptie te voegen, waardoor deze data achteraf kunnen worden geraadpleegd. Verder is gebruikgemaakt van een casestudy protocol (zie paragraaf 2.3), waardoor het onderzoeksproces navolgbaar is. Tot slot zijn de interviews tegen gelezenen zijn meerdere personen geïnterviewd ter controle van eerdere bevindingen.

2.4.2. Ethische aspecten

Om de met dit onderzoek gemoeide ethische aspecten te waarborgen en om er zeker van te zijn dat geen belangrijke uitgangspunten gemist worden, is bij het opzetten van de uitgangspunten met betrekking tot ethiek gebruikgemaakt van de checklist van Saunders (2015).

Algemene ethische kwesties
Algemene ethische kwesties zijn kwesties die van belang zijn voor het gehele onderzoek:

1. Integriteit en objectiviteit
2. Respect
3. Vermijden dat schade wordt toegebracht
4. Privacy
5. Vrijwillige deelname
6. Recht om zich terug te trekken
7. Geïnformeerde toestemming
8. Vertrouwelijkheid en anonimiteit
9. Zich verantwoordelijk gedragen bij analyse en rapportage
10. Naleven van de afspraken over beheer van de gegevens
11. Veiligheid

Daarnaast zijn de volgende maatregelen toegepast:

- Elke deelnemer is geïnformeerd over zijn rechten en het doel van het onderzoek om te voorkomen dat de deelnemer niet op de hoogte is van diens rechten;
- Het onderzoek verwerkt alleen de persoonsgegevens van de deelnemers om ze te kunnen benaderen. Er worden geen andere persoonsgegevens vastgelegd dan die publiekelijk bekend zijn;
- Vanwege ethische aspecten, waaronder geheimhouding en de privacy van de respondenten, zijn er geen persoonsnamen en organisatienamen genoemd in deze scriptie.

3. Theoretisch kader

In dit hoofdstuk wordt het theoretisch kader van het onderzoek gepresenteerd. De theoretische kennis en ideeën die noodzakelijk zijn voor het ontwikkelen van een GDPR *maturity model* worden in kaart gebracht om deelvraag 1 tot en met 4 van dit onderzoek te beantwoorden.

3.1. Onderzoeksaanpak

Voor EA en DM is er gekozen voor een andere onderzoeksaanpak, deze aanpak staat beschreven in dit deelhoofdstuk.

3.1.1. Onderzoeksaanpak EA

Om de eerste deelvraag “Welke maturity models binnen EA kunnen de basis vormen voor een GDPR maturity model?” te kunnen beantwoorden is het van belang te onderzoeken welke *maturity models* er bestaan. De meeste EA *maturity models* worden ontwikkeld door particuliere organisaties en openbare instellingen. Problematisch hierbij is dat deze modellen dikwijls niet worden besproken in traditionele wetenschappelijke literatuur. Er is daarom een alternatieve aanpak gekozen. Middels wetenschappelijke literatuurreviews die een verzameling EA *maturity models* analyseren, wordt aan de hand van de omgekeerde sneeuwbalmethode naar de brondocumenten gezocht. De sneeuwbalmethode houdt in dat publicaties worden gezocht waar andere onderzoekers naar verwijzen. Deze methode is toegepast om het bronmateriaal van de EA *maturity models* terug te vinden

Voor het EA-domein zijn de gebruikte trefwoorden "*enterprise architecture*" en "*maturity model*". Om mogelijke variaties voor "*maturity model*" op te nemen, is ook het synoniem "*maturity framework*" aan de zoekopdracht toegevoegd. Om relevante literatuurreviews op te halen, zijn de sleutelwoorden "*analyse*" (inclusief mogelijke variaties zoals " *analysis*" en "*analyze*") en "*review*" (inclusief "*reviewing*") gebruikt. Er zijn vier selectiecriteria gebruikt bij het zoeken: het moet gaan om literatuurreviews, het gebruik van de Engelse taal, de inhoudelijke relatie met het *maturity model* en de volledige beschikbaarheid van de tekst. Deze criteria zijn opeenvolgend toegepast, wat wil zeggen dat een artikel afviel zodra deze niet aan het eerste criterium voldeed; de rest van de criteria werden dan niet meer expliciet nagegaan. De criteria zijn gebruikt omdat de artikelen verwerkbaar moeten zijn (in het Engels en volledige beschikbaarheid van de tekst), een relatie met het onderzoeksonderwerp moeten hebben (*maturity models*) en een gestructureerde literatuurreview moeten zijn van bestaande EA *maturity models*. Om de kwaliteit van de artikelen te waarborgen is de zoekmachine Web of Science gehanteerd. Publicaties ouder dan tien jaar (van vóór 2008) zijn niet opgenomen om te vermijden dat verouderde informatie in de studie werd verwerkt. Er zijn twee zoekmethoden gebruikt: het zoeken op basis van zoektermen en het gebruik van de sneeuwbalmethode (*snowballing*).

3.1.2. Onderzoeksaanpak DM

Voor het DM-domein worden de volgende zoektermen gebruikt: “*data management*” en “*maturity model*”. Omdat deze zoektermen mogelijke alternatieven kunnen hebben, wordt het synoniem “*maturity framework*” voor “*maturity model*” gebruikt. Bij het zoeken is gebruikgemaakt van vier selectiecriteria, namelijk: het gebruik van de Engelse taal, de inhoudelijke relatie met het *maturity model,* link met DM en de volledige beschikbaarheid van de tekst. Deze criteria zijn gebruikt omdat de artikelen verwerkbaar moeten zijn (Engelse taal en volledige beschikbaarheid van de tekst) en

een relatie met het onderzoeksonderwerp moeten hebben (*maturity models*). Deze criteria zijn opeenvolgend toegepast, wat wil zeggen dat een artikel afviel zodra deze niet aan het eerste criterium voldeed; de rest van de criteria werden dan niet meer expliciet nagegaan. Om de kwaliteit te van de artikelen te borgen zijn alleen gereviewde artikelen gebruikt. Dit is niet expliciet als selectiecriteria opgenomen, omdat de gehanteerde zoekmachine (Web of Science) slechts gereviewde artikelen toont. Publicaties ouder dan tien jaar (vóór 2008) zijn niet meegenomen. Er zijn twee zoekmethoden gebruikt: het zoeken op basis van zoektermen en het gebruik van de sneeuwbalmethode (*snowballing*).

3.2. Uitvoering

3.2.1. Uitvoering EA

De zoektermen voor EA (zie Tabel 1) hebben de in Bijlage 3 genoemde vijftien resultaten opgeleverd. Na toepassing van de selectiecriteria bleven er twee artikelen over: die van Vallerand (2017) en Meyer (2011). Toepassing van de omgekeerde sneeuwbalmethode op deze reviewartikelen heeft een overzicht van elf EA *maturity frameworks* opgeleverd (Zie Bijlage 5). Deze elf EA *maturity frameworks* zijn vervolgens over de onderzoeksgroep verdeeld. Vanuit het onderzoeksteam zijn een tweetal EA *maturity models* toegekend aan dit onderzoek:

- Enterprise Architecture Management Maturity Framework U.S. Government of Accountability Office (United States Government Accountability Office, 2012)
- OMB EA Assessment Framework 3.1, Enterprise Architecture Assessment Framework U.S. Office of Management and Budget (The Office of Management and Budget, 2009)

Zoekmachine	**Zoekterm**	**Aantal resultaten**
Web of Science	("enterprise architecture") and ("maturity model*") or "maturity framework*") *and* ("review*" OR "analy*")	15

Tabel 1. Zoekresultaten EA

3.2.2. Uitvoering DM

De zoektermen voor DM hebben de resultaten als weergegeven in Tabel 2 opgeleverd. Deze resultaten zijn getoetst aan de volgende vier selectiecriteria: tekst in het Engels, relatie tot een *maturity model*, link met DM en volledige beschikbaarheid van de tekst. De toepassing van deze selectiecriteria is in Bijlage 4 uiteengezet, wat één relevant model heeft opgeleverd, namelijk:

- MD3M: The master data management maturity model (Spruit & Pietzka, 2014).

Toepassing van de omgekeerde sneeuwbalmethode op het MD3M-artikel heeft geresulteerd in twee aanvullende modellen:

- Data management Capability maturity Model (DCAM), (DAMA, 2014)
- Data Management Maturity (DMM), (CMMI institute, 2014)

Zoekmachine	Zoekterm	Aantal resultaten
Web of Science	("maturity model" OR "maturity framework") AND ("data management")	5

Tabel 2. Zoekresultaten DM

3.3. Resultaten

Ter beantwoording van de tweede deelvraag "Welke kernaspecten van GDPR-maturity kunnen worden afgeleid uit *maturity models* binnen EA en DM?" zijn eerst de kernaspecten van de GDPR in kaart gebracht. Vervolgens zijn de verschillende EA en DM *maturity models* kort beschreven en is er een koppeling gemaakt tussen deze modellen en de GDPR-kernaspecten. Op basis van de aspecten uit EA en DM *maturity models* is een *maturity model* ontworpen dat gericht is op de GDPR.

3.3.1. Kernaspecten GDPR

In paragraaf 1.1 is het doel van de GDPR beschreven. Schermer beschrijft zes kernaspecten van de GDPR (Schermer et al., 2018, p. 15). Deze kernaspecten zijn verdeeld in het opslaan (Tabel 3) en de verwerking van gegevens (Tabel 4).

Beschrijving	Kernwoord (en)
De gegevens moeten goed beveiligd zijn en vertrouwelijk blijven	Integriteit en vertrouwelijkheid
De gegevens mogen niet langer worden bewaard dan nodig	Opslagbeperking
De gegevens moeten juist zijn	Juistheid

Tabel 3. GDPR-kernaspecten voor het opslaan van persoonsgegevens

Beschrijving	Kernwoord (en)
De verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn	Rechtmatigheid, behoorlijkheid, transparantie
De verwerking moet gebonden zijn aan specifieke verzameldoelen	Doelbinding
De persoonsgegevens moeten toereikend zijn, ter zake dienend, en beperkt tot wat noodzakelijk is.	Minimale gegevensverwerking

Tabel 4. GPDR-kernaspecten over het verwerken van persoonsgegevens

3.3.2. Resultaten EA

Enterprise Architecture Management Maturity Framework U.S. Government of Accountability Office (GOA 2.0)

Sinds het begin van de jaren negentig heeft de U.S. Government of Accountability Office (GOA) het gebruik van EA als essentiële toepassing beschouwd om goed gebruik van technologie te maximaliseren. Goed gebruik van technologie werd behaald door kostenbesparing, hergebruik van diensten en het delen en het standaardiseren van data. Om nationale overheden in de ontwikkeling van EA bij te staan is in 2002 de eerste versie van het GOA *framework* uitgegeven. In 2009 is deze opgevolgd door versie 2.0. Het *framework* gebruikt kritische prestatie indicatoren (KPI's) om de EA *maturity* vast te stellen. Deze KPI's zijn opgedeeld in drie deelgebieden, te weten: compleetheid, gebruik en resultaten. De mate van *maturity* wordt weergegeven in zeven *levels*, zoals weergegeven in Bijlage 6. De KPI's worden uitgedrukt in beoordelingen van één tot vijf. Het framework scoort op basis van 59 elementen onderdeel van 15 attributen verdeeld over 4 domeinen. De attributen zijn weergegeven en gekoppeld aan de GDPR-kernaspecten in Bijlage 7. Bij het ontbreken van een relatie met een GDPR-kernaspect is dit weergegeven met 'geen'. 8 van de 15 attributen zijn te koppelen aan een GDPR-kernaspect. Binnen het domein "EA management vertegenwoordiging" zijn dit: *demonstratie van commitment* (1) en v*oorzien in middelen om commitment te bereiken* (2). Binnen functionele EA-vertegenwoordiging zijn dit: *governance* (3) en *gebruik* (4). Binnen OMB gebiedsvertegenwoordiging zijn dit: *compleetheid* (5)*, gebruik* (6) en *resultaten* (7). Binnen EA als enabler is dit het attribuut *processen* (8).

OMB EA Assessment Framework 3.1

Het OMB EA Assessment Framework is ontwikkeld door de U.S. Office of Management and Budget. Het *framework* identificeert meetgebieden voor het effectief gebruik van EA, zodat het *framework* gebruikt kan worden om de prestaties van een organisatie te verbeteren. Toepassing resulteert in vijf concrete resultaten, namelijk: prestatiekloven dichten, kostenbesparing, kwaliteitsverbetering, datakwaliteit en verbetering van beschikbaarheid, deelbaarheid en transparantie. Het *framework* wordt gebruikt voor zelfbeoordeling gedurende het jaar met een eindbeoordeling door OMB. Doel van dit *maturity model* is het vinden van zwakke plekken in EA en het ontwikkelen van een plan om deze te verbeteren. Het model hanteert vijf *maturity levels*: van niveau één (laagste niveau) tot niveau vijf (hoogste niveau). Deze *levels* worden verder niet geduid. De prestaties worden gemeten op drie gebieden: compleetheid, gebruik en resultaten. Deze gebieden zijn opgedeeld in deelgebieden die specifiek worden getoetst.

In Bijlage 8 zijn de deelgebieden weergegeven en waar mogelijk gekoppeld aan de kernaspecten van de GDPR. Als er geen relatie is met een GDPR-kernaspect is dit met 'geen' weergegeven. Eén deelgebied, *samenwerking en hergebruik* (1), is gekoppeld aan een GDPR-kernaspect.

3.3.3. Resultaten DM

Master Data Management Maturity Model (MD3M)

Het doel van MD3M is om de volwassenheid van de masterdata te meten. MD3M definieert masterdata als data die de meest relevante bedrijfsentiteiten (zoals producten of werknemers) beschrijven, waarop een organisatie haar activiteiten baseert. MD3M bestaat uit vijf focusgebieden en vijf volwassenheidslevels (Spruit & Pietzka, 2014). Deze focusgebieden zijn: *data model*, *data quality, usage and ownership, data protection* en *maintenance*. Binnen *data model* worden de data

vanuit het perspectief van de organisatie en de infrastructuur bekeken, bijvoorbeeld door na te gaan hoe data gestructureerd zijn en uit welke systemen ze komen. Binnen *data quality* wordt gekeken hoe de kwaliteit van data gemeten en verbeterd kan worden. Binnen *usage and ownership* wordt onderzocht welke data gebruikt worden binnen welk systeem. Hoe data beveiligd worden, wordt binnen *data protection* onderzocht. Binnen *maintenance* wordt bezien hoe data opgeslagen worden en hoe die gebruikt worden binnen de *lifecycle* (Spruit & Pietzka, 2014). In Bijlage 9 zijn de verschillende volwassenheidslevels weergegeven. Elf basisbeginselen, te weten: *master data model* (1), *data landscape* (2), *assessment of data quality* (3), *awareness of quality gaps* (4), *data usage* (5), *data ownership* (6), *data access* (7), *improvement* (8), *data protection* (9), *storage* (10) en *data lifecycle* (11) hebben een relatie tot een GDPR-kernaspect. In Bijlage 10 zijn deze weergegeven met een aanvullende motivatie.

Data Management Capability Assessment Model (DCAM)

Het Data Management Capability Assessment Model definieert de vereiste vaardigheden om DM binnen een organisatie mogelijk te maken en te ondersteunen. DCAM adresseert de DM-strategie, de organisatiestructuren, de technologie en de operationele *best practices* die nodig zijn om succesvol te zijn op het vlak van DM. DCAM bestaat uit kerncomponenten, waarbij elke component wordt gedefinieerd door een reeks vereiste beheermogelijkheden. Elke mogelijkheid wordt ondersteund door een reeks submogelijkheden, doelstellingen, implementatieadviezen en voorbeelden van bewijsmateriaal die nodig zijn om de prestaties te verifiëren. In Bijlage 11 zijn de kerncomponenten weergegeven en gekoppeld aan de GDPR-kernaspecten. De volwassenheidsniveaus verschillen hierbij per kerncomponent, variërend van twee (*data operations program*) tot zeven (*data management strategy* en *data governance*). De zes kerncomponenten *data management* (1) *strategy* (2), *data governance* (3), *data architecture* (4), *technology architecture* (5) en *data quality* (6) zijn gekoppeld aan een GDPR-kernaspect.

Data Management Maturity Model (DMM)

Het DMM bestaat uit een raamwerk van gegevensbeheerpraktijken in zes hoofdcategorieën. Hiermee kunnen organisaties de eigen capaciteiten benchmarken, sterke punten en hiaten identificeren en de data gebruiken om de prestaties te verbeteren. De DMM domeinen zijn in Bijlage 13 gekoppeld aan de GDPR-kernaspecten. Alle hoofdcategorieën, te weten: *data management strategy* (1)*, data quality* (2)*, data operations* (3) *, platform and architectures* (4)*, data governance* (5) en *supporting processes* (6) zijn gekoppeld aan een GDPR-kernaspect. Het model kent vijf *maturity levels*, namelijk: *initial level, managed level, defined level, quantitative managemen*t *level* en optimization *level*, zoals weergegeven in Bijlage 12.

3.4. Maturity levels

Ter beantwoording van de derde deelvraag “Welke volwassenheidsniveaus zijn nodig voor het beschrijven van volwassenheid voor de GDPR?” worden binnen deze paragraaf de volwassenheidsniveaus van de vijf geanalyseerde *maturity models* vergeleken. Na analyse van de volwassenheidsniveaus worden de verschillende niveaus tegen elkaar afgezet en in Tabel 6 weergeven. Deze niveaus zijn de input voor de volwassenheidsniveaus van het nieuwe GDPR-volwassenheidsmodel.
De vijf volwassenheidsmodellen die met elkaar vergeleken zijn, zijn:

- Enterprise Architecture Management Maturity Framework U.S. Government of Accountability Office (United States Government Accountability Office, 2012)
- OMB EA Assessment Framework 3.1, Enterprise Architecture Assessment Framework U.S. Office of Management and Budget (The Office of Management and Budget, 2009)
- MD3M: The master data management maturity model (Spruit & Pietzka, 2014)
- Data management Capability maturity Model (DCAM), (DAMA, 2014)
- Data Management Maturity (DMM), (CMMI institute, 2014)

Het resultaat van de analyse is weergegeven in Bijlage 19, waarin de verschillende volwassenheidsniveaus met elkaar zijn vergeleken. Iedere kolom representeert een volwassenheidsmodel. Binnen het OMB 3.1-model zijn de verschillende niveaus niet omschreven, maar genummerd weergegeven in niveaus van één (laagste niveau van volwassenheid) tot en met vijf (hoogste niveau van volwassenheid). De GOA 2.0 kent als enige van de vijf modellen zeven volwassenheidsniveaus die fijnmazig zijn beschreven. Om deze reden zijn de twee hoogste niveaus samengevoegd in niveau vijf.

Op niveau nul is nog geen sprake van awareness; die moet nog worden gecreëerd (GOA 2.0). Op het eerste niveau is sprake van het eerste bewustzijn (MD3M): de eerste initiatieven vinden plaats maar deze zijn ad hoc (OMB 3.1). Op niveau twee zijn fundamenten aanwezig die zich bevinden op proces- of medewerkersniveau (MD3M). Op het derde niveau worden initiatieven gekoppeld aan organisatiedoelstellingen en is sprake van standaardprocessen die zijn beschreven (DMM). Niveau vier wordt gekenmerkt door de integratie in de organisatie (DCAM), door de aanwezigheid van standaarden en door de aanwezigheid van metingen en criteria. Het hoogste niveau – vijf – wordt gekenmerkt door doorontwikkeling (GOA 2.0) en analyse van de resultaten.

Iedere categorisatie is vertaald naar een volwassenheidsniveau dat gebruikt kan worden in het GDPR *maturity model*. In Tabel 5 is een overzicht weergegeven van de *maturity levels* van het GDPR *maturity model*.

Maturity level	**Beschrijving**
0. afwezig	Het *maturity*-aspect is afwezig binnen de organisatie en er zijn geen initiatieven om deze te ontplooien. Er is geen plan of budget om deze te ontwikkelen (United States Government Accountability Office, 2012).
1. Initieel	Er is sprake van een eerste bewustzijn (Spruit & Pietzka, 2014). De eerste initiatieven voor de ontwikkeling van het deelgebied worden in gang gezet. De getroffen maatregelen zijn ad hoc (The Office of Management and Budget, 2009).
2. Basic	De eerste fundamenten van het deelgebied zijn aanwezig, deze bevinden zich op basisproces- of medewerkersniveau (Spruit & Pietzka, 2014) en hangen niet samen met organisatiedoelstellingen.
3. Managed	Initiatieven zijn gekoppeld aan organisatiedoelstellingen. Processen en procedures gerelateerd aan het *maturity*-aspect zijn beschreven (CMMI institute, 2014). De organistie heeft een actieve rol in de ontwikkeling van het deelgebied.
4. Geoptimaliseerd	Het *maturity*-aspect maakt onderdeel uit van de organisatie, wordt door de organisatie gemeten en is gebaseerd op standaarden (United States Government Accountability Office, 2012) .
5. Continu verbeterd	Het *maturity*-aspect wordt continu gemonitord en verbeterd (United States Government Accountability Office, 2012). Er vindt toetsing plaats van het *maturity*-aspect.

Tabel 5. Maturity levels GDPR *maturity model*

3.5. GDPR *maturity model*

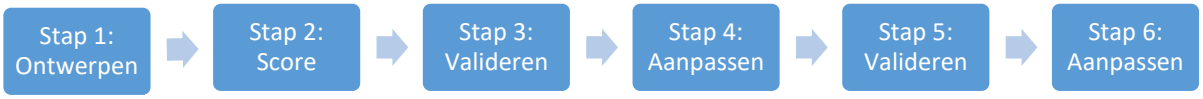
Met het opstellen van het GDPR *maturity model* wordt invulling gegeven aan de vierde deelvraag, luidende: “Welke criteria zijn nodig voor het beschrijven van het maturity level van de GDPR aspecten?” Criteria voor het betreffende *maturity level* zijn beschreven in de verschillende cellen van het model in Tabel 6. Om het nieuwe model vorm te geven zijn de kernaspecten uit de gehanteerde EA en DM-modellen opgenomen onder de betreffende kolom in Bijlage 14. Daar waar een relatie tot de GDPR ontbrak is ‘geen’ opgenomen. Bij het ontbreken van het betreffende beschrijvende niveau is een ‘*’ opgenomen. Vervolgens zijn deze kernaspecten samengevoegd tot de nieuwe kernaspecten van het GDPR-volwassenheidsmodel, als beschreven in Tabel 6. Hierbij zijn er per GDPR-kernaspect niveaus van volwassenheid ingevuld. Deze niveaus zijn uitgedrukt in specifieke eisen die zijn weergegeven in de verschillende cellen van de tabel. Door middel van bronvermelding is de koppeling met de EA en DM *maturity models* kort weergegeven.

Maturity level	**0. Afwezig**	**1. Initieel**	**2. Basic**	**3. Managed**	**4. Geoptimaliseerd**	**5. Continu verbeterd**
GDPR-kernaspecten						
Integriteit en vertrouwelijkheid	Aandacht voor integriteit en vertrouwelijkheid van persoonsgegevens is afwezig	Aan de technische eisen van beveiliging van persoonsgegevens is voldaan (Spruit & Pietzka, 2014). Nieuwe oplossingen die persoonsgegevens verwerken worden getoetst aan deze standaarden (CMMI institute, 2014)	Er wordt gelogd wie toegang heeft tot persoonsgegevens en er is een datamanagement strategie (CMMI institute, 2014)	Toegang tot persoonsgegevens wordt op basis van *rules* verstrekt. (Spruit & Pietzka, 2014). Er is aandacht voor rationalisatie van persoonsgegevens (CMMI institute, 2014)	Beveiligingsbeleid berust op standaarden en er is een datamanagementstrategie (DAMA, 2014), Er is bewustzijn onder medewerkers voor informatiebeveiliging	Informatiebeveiliging wordt continu doorontwikkeld en verbeterd (CMMI institute, 2014)
Opslagbeperking	Aandacht voor opslagbeperking van persoonsgegevens is afwezig	Data is logisch opgeslagen, de organisatie is bekend met data *lifecycle management* (CMMI institute, 2014)	Opgeslagen persoonsgegevens worden gecontroleerd (CMMI institute, 2014). Data is logisch opgedeeld in domeinen. (DAMA, 2014)	Er is regelmatig controle op de noodzaak van het opslaan van persoonsgegevens (Spruit & Pietzka, 2014)	Er is sprake van één source of truth voor persoonsgegevens. Persoonsgegevens worden enkelvoudig opgeslagen (Spruit & Pietzka, 2014)	Persoonsgegevens zijn op innovatieve wijze opgeslagen en er wordt gelogd door wie deze gegevens worden geraadpleegd (Spruit & Pietzka, 2014)
Juistheid	Aandacht voor juistheid van persoonsgegevens is afwezig	Er is binnen de organisatie bewustzijn voor de juistheid van gegevens (Spruit & Pietzka, 2014) en er zijn standaarden voor datakwaliteit (CMMI institute, 2014)	Er is binnen de organisatie een begrip voor juistheid van gegevens (Spruit & Pietzka, 2014). Er is een strategie voor datakwaliteit (DAMA, 2014)	De juistheid van persoonsgegevens wordt getoetst (DAMA, 2014). Er wordt invulling gegevens aan de strategie voor datakwaliteit (CMMI institute, 2014)	De juistheid van gegevens wordt getoetst en aan de uitkomsten wordt opvolging gegeven (CMMI institute, 2014). Datakwaliteit wordt gemeten en hier wordt over gerapporteerd (Spruit & Pietzka, 2014)	Juistheid van gegevens wordt vergeleken met andere partijen (CMMI institute, 2014) en er is sprake van continue doorontwikkeling (United States Government Accountability Office, 2012)
Rechtmatigheid, behoorlijkheid en transparantie	Aandacht voor rechtmatigheid, behoorlijkheid en transparantie is afwezig	Eigenaarschap van gegevens is vastgelegd (United States Government Accountability Office, 2012) en er is zicht op wie welke gegevens gebruikt	Eigenaarschap van gegevens is vastgelegd en dit wordt gecommuniceerd. Er is sprake van *data governance* (CMMI institute, 2014)	*Data governance* is organisatiebreed ingericht (CMMI institute, 2014) en persoonsgegevens zijn alleen toegankelijk indien dat strikt noodzakelijk is (Spruit & Pietzka, 2014)	Er is zicht op al het datagebruik binnen de organisatie (Spruit & Pietzka, 2014) en dit gebruik wordt gecommuniceerd	*Data governance* is organisatiebreed ingericht (DAMA, 2014) en wordt continu verbeterd (United States government accountability office, 2012)
Doelbinding	Aandacht voor doelbinding is afwezig	Er is een basisdefinitie voor doelbinding binnen de organisatie (Spruit & Pietzka, 2014)	Er is een datamanagementstrategie waarin doelbinding wordt geadresseerd (CMMI institute, 2014)	Inzicht voor welke doelen persoonsgegevens worden verzameld en welke doel aan welke data is gekoppeld (DAMA, 2014)	Persoonsgegevens die niet aan een doel te koppelen zijn worden actief verwijderd (CMMI institute, 2014)	Doelbinding van persoonsgegevens wordt continu doorontwikkeld (CMMI institute, 2014)
Minimale gegevensverwerking	Aandacht voor minimale gegevensverwerking is afwezig	Er is een definitie voor minimale gegevensverwerking (The Office of Management and Budget, 2009)	Er is bekend wie welke gegevens binnen een organisatie kan verwerken	Er is bekend of persoonsgegevens (rechtmatig) worden gebruikt (CMMI institute, 2014)	Persoonsgegevens die niet worden gebruikt worden verwijderd (CMMI institute, 2014)	Minimale gegevensverwerking wordt continu doorontwikkeld

Tabel 6. GDPR *maturity levels*

4. Resultaten

Om antwoord te geven op de vijfde deelvraag “Hoe kan het *maturity model* in de praktijk worden gevalideerd?” zijn er binnen dit onderzoek twee interactieve cycli uitgevoerd voor de ontwikkeling van het model (stap drie tot en met zes in Figuur 3). Er is gekozen voor twee cycli vanwege de beperkte tijd die voor dit onderzoek staat. Om het in hoofdstuk 3 ontworpen GDPR m*aturity model* te kunnen valideren is deze eerst toegepast (stap twee in Figuur 3) waarbij een volwassenheidsniveau is vast gesteld. Dit is gedaan door het model af te nemen door middel van de vragenlijst, afgeleid uit het model (Bijlage 15).



Figuur 3. Schematische weergave van ontwikkelstappen

De algemene geschiktheid van het model is vervolgens kwantitatief getoetst op van nut en gebruiksgemak (stap drie, Figuur 3) door gebruik te maken van de TAM-vragenlijst van Davis (1989). De inhoud van het model, in de vorm van de afgeleide vragen, is voorgelegd aan de respondenten. Hierbij is gevraagd naar mate waarin de vragen uit de vragenlijst relevant zijn om een GDPR-aspect te beschrijven, uitgedrukt in een zevenpunts-Likertschaal. Ten slotte is ook gevraagd naar de algemene tevredenheid van de respondenten over het model. Deze vragen hebben als input gediend voor de middels een semigestructureerd interview verkregen kwalitatieve feedback. Vervolgens zijn de vragen en het model aangepast (stap vier, Figuur 3) en heeft er een tweede evaluatiecyclus plaatsgevonden (stap vijf en zes, Figuur 3).

Hiermee is invulling gegeven aan de Design Science-methodologie, doordat het artefact (het *maturity model*) en één instantie (het toegepaste GDPR *maturity model)* zijn opgesteld en doorontwikkeld. Voor het toepassen van het model zijn twee verschillende experts parallel bevraagd over het model. Beide experts zijn betrokken bij de implementatie van de GDPR binnen de eigen organisatie en hebben een functie als GDPR-adviseur. Om op te kunnen treden als subject (expert) in deze studie hebben zij kennis van de GDPR en de implementatie daarvan in de eigen organisatie nodig. De experts zijn werkzaam bij twee grote publieke organisaties, met respectievelijk 58.000 (organisatie één) en 3.000 (organisatie twee) medewerkers. Ter evaluatie van het model zijn twee aanvullende experts met een vergelijkbare rol binnen organisatie één betrokken.

4.1. GDPR maturity vragenlijst

Het model is eerst toegepast door semigestructureerde interviews bij de twee experts van de twee organisaties af te nemen. Hiervoor is gebruikgemaakt van een vooraf opgestelde vragenlijst (Bijlage 15) gebaseerd op de verschillende deelgebieden van het GDPR-model teneinde de vragenlijst makkelijker toepasbaar te maken voor de gebruiker. De vragenlijst is gebaseerd op Bijlage 14, waarin een integraal overzicht wordt geboden van de relatie van de verschillende *maturity models* tot de GDPR. Uit de modellen zijn statements (korte beschrijvingen van het betreffende niveau, te relateren aan de GDPR) samengevoegd tot een afgeleid GDPR-statement. Als laagste niveau (niveau nul) is een statement opgenomen dat de totale afwezigheid van aandacht voor het betreffende deelgebied uitdrukt. Deze statements zijn vertaald naar de vragen in Bijlage 15, in Tabel 7 is dit weergegeven voor de GDPR-kenaspecten integriteit en vertrouwelijkheid. De statements zijn vertaald naar interviewvragen met antwoordopties. Het betreffen ja-nee antwoordopties of meerkeuzevragen waarvoor het antwoord in bepaalde klassen dient te worden uitgedrukt. Een voorbeeld van een antwoord in een klasse vormt vraag drie bij het deelgebied doelbinding. Afwezigheid van doelbinding in datamanagementstrategie leidt tot vaststelling van niveau twee. Vastlegging van doelbinding voor persoonsgegevens voor bepaalde datagroepen leidt tot vaststelling van niveau drie en een vervolgvraag voor vaststelling van niveau vier.

De lijst bevat vragen met een scoring en voorwaardelijkheid. Een bevestigend antwoord op de vraag leidt tot het groeien in niveau; men gaat dan door naar de volgende vraag. Bij het niet “halen” vindt de vaststelling van een *maturity level* op het deelgebied plaats. Bij het niet halen van een laag niveau worden de aspecten op hogere niveaus dus niet meer bevraagd.

Integriteit en vertrouwelijkheid	
Afgeleid GDPR-statement	*Afgeleide vraag*
Aandacht voor integriteit en vertrouwelijkheid van persoonsgegevens is afwezig	Is er binnen de organisatie aandacht voor de Integriteit en vertrouwelijkheid van persoonsgegevens?
Aan de technische eisen van de beveiliging van persoonsgegevens is voldaan. Nieuwe oplossingen die persoonsgegevens verwerken worden getoetst aan deze standaarden	Zijn er binnen uw organisatie standaarden gericht op integriteit en vertrouwelijkheid voor implementatie van nieuwe dataoplossingen, en zo ja, welke zijn dit?
Er wordt gelogd wie toegang heeft tot persoonsgegevens en er is een datamanagementstrategie	Is er logging van het raadplegen of muteren van gegevens binnen de organisatie ingericht?
Toegang tot persoonsgegevens wordt op basis van rules verstrekt en er is aandacht voor rationalisatie van persoonsgegevens	Wordt toegang tot persoonsgegevens op basis van rollen verstrekt?
Beveiligingsbeleid berust op standaarden en er is een datamanagementstrategie. Er is bewustzijn onder medewerkers over informatiebeveiliging	Zijn medewerkers zich bewust van informatiebeveiliging? Wat voor maatregelen zijn er door de organisatie genomen om dit bewustzijn te waarborgen?
Er is constant aandacht voor beveiliging van gegevens en lessen worden gedeeld	Hoe wordt er door de organisatie geleerd op het gebied van informatiebeveiliging en hoe worden deze lessen gedeeld?

Tabel 7. GDPR-statements en afgeleide vragen

4.2. Vaststellen *maturity*-niveau

Voor het vaststellen van het *maturity*-niveau van de twee organisaties is er per organisatie één interview afgenomen. Daartoe is de gestructureerde vragenlijst doorlopen waarbij er een scoring per deelgebied is gegeven. Dit heeft geresulteerd in de scoring die is weergeven in Tabel 8. De scoring is als input meegegeven aan de respondenten voor het tweede interview, waarbij het model is geëvalueerd.

GDPR- kernaspecten	0. afwezig	1. Initieel	2. basis	3. Managed	4. geoptimaliseerd	5. continu verbeterd
Integriteit en vertrouwelijkheid						1, 2
Opslagbeperking		2				1
Juistheid					2	1
Rechtmatigheid, behoorlijkheid, transparantie					2	1
Doelbinding					1, 2	
Minimale gegevensverwerking				2	1	

Tabel 8. Maturity score

4.3. Eerste iteratie

4.3.1. TAM-scoring

De experts zijn gevraagd naar de verwachte bruikbaarheid en het gebruiksgemak van het aan de hand van de TAM-vragenlijst (Davis, 1989). Een overzicht van de score per deelgebied is weergegeven in Tabel 9. Dit overzicht ziet op de deelgebieden verwachte bruikbaarheid, het verwachte gebruiksgemak en de intentie voor gebruik. In Bijlage 18 zijn alle gegevens inzichtelijk gemaakt. De vragenlijst bevat negatieve stellingen: van deze stellingen is de score omgedraaid om tot een correcte waarde te komen. Deze input is geclusterd per deelgebied. In de interviews heeft een verdere kwalitatieve verdieping op basis van de TAM-scoring plaatsgevonden, hiervan is een korte samenvatting opgenomen.

	Organisatie 1, Respondent 1	Organisatie 1, Respondent 2	Organisatie 1, Respondent 3	Organisatie 2	Gemiddelde score
Verwachte bruikbaarheid (Perceived Usefulness, PU)	4,9	4,3	4,37	4,5	4,5
Verwacht gebruiksgemak (Perceived Ease of Use, PEOU)	5,7	5,3	5,8	6	5,7
Intentie voor gebruik (Intention to use, IU)	5,5	5	4,5	5	5

Tabel 9. Samenvatting TAM-scores

Kwalitatieve feedback TAM

Verwachte bruikbaarheid

De respondenten gaven aan dat het *maturity model* goed te gebruiken is voor inhoudelijk betrokkenen, oftewel personen die al betrokken zijn bij de GDPR. Voor niet-betrokkenen personen is het model te technisch, vanwege het gebruik van jargon. Het model biedt verder te weinig differentiatiemogelijkheden. In de praktijk komt het immers weinig voor dat een organisatie volledig wel of niet voldoet aan de GDPR; de GDPR is vaak slechts van toepassing op een deel van de applicaties of domeinen. Om de herkenbaarheid te vergroten is tot slot het beter Nederlandse termen te gebruiken voor het beschrijven van niveaus.

Verwacht gebruiksgemak

De respondenten gaven aan dat het model niet ingewikkeld is of moeilijk te begrijpen, maar het model is tamelijk globaal en biedt daarom niet direct inzicht in waar er verbetermogelijkheden zijn. Toepassing van de GDPR wordt wel gemakkelijker door gebruik van het model, maar geeft niet direct inzicht in waar op technisch niveau maatregelen moeten worden genomen. Het model kan dus dienst doen in de gereedschapskist van modellen en tools.

Intentie voor gebruik

De respondenten geven aan dat er al veel modellen beschikbaar zijn voor informatiebeveiliging en privacy. Dit model komt daar nog eens bij. Daarnaast zijn dit soort modellen met name nuttig voordat men begint met het treffen van maatregelen, dus als een nulmeting (dit is echter niet de fase waar beide organisaties zich in bevinden). Het model is goed bruikbaar bij nieuwe processen of organisatieonderdelen, maar leent zich dus minder voor bestaande processen of organisatieonderdelen, omdat hier reeds maatregelen zijn genomen.

4.3.2. Delphi-studie

Na het vaststellen van het *maturity model* is de Delphi-techniek toegepast om de vragen van het model te evalueren. De vragen van het model zijn voorgelegd aan de vier experts) middels een vragenlijst. De vragen zijn beoordeeld op basis van relevantie aan de hand van een zevenpunts-Likertschaal. De evaluatie van de inhoud van de vragen heeft geleid tot het aanpassen van negen en het schrappen van één van de 35 vragen. De hoeveelheid aangepaste vragen per categorie is weergegeven in Tabel 10. In Bijlage 20 is een complete scoring weergegeven met de scoring en stabiliteit per scoringsvraag. Naast de scoring per vraag is een gemiddelde algemene tevredenheidsscoring van een zeven uit tien toegekend door respondenten (Bijlage 22).

GDPR-categorie	Aantal vragen	Gemiddelde score vragen categorie (1-7)	Behouden vragen	hoeveelheid aangepaste vragen
Integriteit en vertrouwelijkheid	6	6,1	6	0
Opslagbeperking	6	5,8	5	1
Juistheid	6	5,1	1	5
Rechtmatigheid, behoorlijkheid, transparantie	7	6	6	1 (verwijderd)
Doelbinding	5	5,5	5	0
Minimale gegevensverwerking	5	5,6	2	3

Tabel 10. Gewijzigde vragen per categorie

In de interviews heeft een verdere kwalitatieve verdieping plaatsgevonden op de negatieve scores (scores onder de zes) voor de vragen van de vragenlijst van het volwassenheidsmodel. Daarnaast zijn nog een aantal open vragen gesteld over de toepassing van en mogelijke verbeteringen voor het model. De interviews hebben geresulteerd in de input, samengevat per GDPR-kernaspect Tabel 11. Deze feedback is cursief tussen haakjes in verschillende klassen opgedeeld. Deze klassen komen terug als motivatie bij de aanpassing van de vragen.

GDPR-kernaspect	Samenvatting input interviews
Integriteit en vertrouwelijkheid	Producten zoals PIA's en verwerkersovereenkomsten kunnen van waarde zijn (*producten benoemen)*. Producten en functies (organisatorische kant) laten terugkomen maakt het model herkenbaar. Producten zijn goed herkenbaar en daarmee goed te meten.
Opslagbeperking	Breng onderscheid aan in daadwerkelijk verwijderen (archiving) en vernietigen (purging) *(verwijderen en vernietigen)*.
Juistheid	Benchmarking levert relatief weinig op voor ons. Vergelijken van verschillende organisaties is lastig, de omgevingen en taken kunnen erg verschillend zijn (*benchmarking*).
Rechtmatigheid, behoorlijkheid, transparantie	Wat er nog ontbreekt is het beleggen van rollen (de organisatorische inrichting) (*rollen benoemen*). Daarnaast is er geen aandacht voor de verwerkersovereenkomst (*producten benoemen)*. De rechten van betrokkenen worden in de wet expliciet benoemd, maar komen niet expliciet terug in het model (*rechten van betrokkenen)*.
Doelbinding	Definities doen er minder toe en deze komen direct uit de AVG (*definities schrappen*). Doelbinding wordt vastgelegd in een verwerkingsregister. Hier kan beter gericht naar worden gevraagd (*producten benoemen)*.
Minimale gegevensverwerking	Definities liggen vast in de AVG (*definities schrappen*).

Tabel 11. Input uit interviews per GDPR-*kernaspect*

De vragen in Tabel 12 zijn de vragen waarbij geen sprake was van consensus of stabiliteit. Deze zijn gewijzigd (of in één geval geschrapt) op basis van de verkregen kwalitatieve feedback. De feedback op basis waarvan deze vraag is aangepast is tussen haakjes weergegeven. Het volwassenheidsniveau 'basic' is op basis van de feedback aangepast naar 'basis'.

Originele vraag	Aangepaste vraag
Wordt de opslag van persoonsgegevens op relevantie gecontroleerd? (is het doel waarvoor de gegevens zijn verworven nog steeds van toepassing)	Zijn de persoonsgegevens die worden verwerkt vastgesteld in een verwerkingsregister? (*producten benoemen*)
Zijn medewerkers zich bewust van deze standaarden?	Wordt de juistheid van persoonsgegevens bewaakt en is er de mogelijkheid persoonsgegevens te corrigeren? (*rechten van betrokkenen*)
Is er een bewuste strategie voor datakwaliteit?	Wordt de juistheid van persoonsgegevens organisatiebreed op een eenduidige wijze bewaakt en formeel vastgesteld? (*rechten van betrokkenen)*

Vindt er toetsing van de juistheid van persoonsgegevens plaats (bijvoorbeeld door vergelijking met de informatiebron) en worden er acties ondernomen bij het constateren van onjuiste gegevens?	Is de juistheid van persoonsgegevens door de keten heen gegarandeerd? (*rechten van betrokkenen)*
Is er een strategie voor het verbeteren van de datakwaliteit?	Maakt de kwaliteit van persoonsgegevens integraal onderdeel uit van de management- en architectuurprocessen? (*rechten van betrokkenen)*
Is er sprake van benchmarking door de juistheid van gegevens te vergelijken met andere organisaties?	Stuurt het hoogste management op het bewaken van de juistheid van persoonsgegevens? (*rechten van betrokkenen)*
Is *data governance* binnen de organisatie ingericht?	Geschrapt
Welke definitie wordt er binnen de organisatie gehanteerd voor minimale gegevensverwerking?	Zijn de verplichte AVG-rollen (zoals een FG) aanwezig binnen de organisatie en zien deze toe op minimale gegevensverwerking? (*definities schrappen*) (*rollen benoemen*)
Hoe is het toezicht op de rechtmatige verwerking van gegevens ingericht?	Vindt het bepalen en omschrijven van de verzameldoeleinden en de rechtvaardigingsgronden organisatiebreed op een eenduidige formele manier plaats? (*producten benomen*)
Op welke wijze worden persoonsgegevens verwijderd nadat zij doelbindingen hebben verloren en hoe wordt dit gecontroleerd?	Worden de bepaalde en omgeschreven verzameldoeleinden en rechtvaardigingsgronden vergeleken met gelden gronden van vergelijkbare organisaties? (*benchmarking)*

Tabel 12. Aangepaste scoringsvragen

4.4. Tweede iteratie

Na aanpassing van het GDPR m*aturity model* en de bijbehorende interviewvragen zijn de aangepaste vragen opnieuw middels een vragenlijst uitgezet bij de vier experts. Hierop is een complete terugkoppeling ontvangen van drie van de vier experts, weergeven per categorie in Tabel 13. Dit heeft bij vier van de negen aangepaste vragen geresulteerd in een algemene consensus (Bijlage 21) en bij vier aanvullende vragen tot stabiliteit op basis van de kappa-score om de vragen te behouden. Bij één vraag – o*p welke wijze worden persoonsgegevens verwijderd nadat zij doelbindingen hebben verloren en hoe wordt dit gecontroleerd?* – is geen sprake van consensus of stabiliteit. Deze vraag is onderdeel van minimale gegevensverwerking en had een gemiddelde score van een vier. Een dergelijke score vraagt om het aanpassen of verwijderen van deze vraag. Gelet op de beperkte tijd die voor dit onderzoek staat konden slechts twee iteraties worden uitgevoerd. Er heeft daarom geen verdere aanpassing van deze vraag plaatsgevonden en er is ter zake geen kwalitatieve feedback verzameld.

De algemene tevredenheidsscore is met een halve punt toegenomen tot een 7,5 (Bijlage 22). Vanwege tijdsgebrek is het model niet verder doorontwikkeld. De aanpassingen resulteren in een aangepast GDPR m*aturity model* dat is weergeven in Bijlage 23.

GDPR-categorie	Aantal aangepaste vragen	Gemiddelde score vragen categorie (1-7)
Integriteit en vertrouwelijkheid	0	NVT
Opslagbeperking	1	6
Juistheid	5	5.9
Rechtmatigheid, behoorlijkheid, transparantie	1 (verwijderd)	NVT
Doelbinding	0	NVT
Minimale gegevensverwerking	3	5.4

Tabel 13. Scoring gewijzigde vragen per categorie

5. Discussie, conclusies en aanbevelingen

Dit hoofdstuk bevat de discussie en conclusie van dit onderzoek. Verder worden enkele aanbevelingen voor vervolgonderzoeken gedaan en vindt een inhoudelijke methodologische reflectie op de kwaliteit van het gevolgde onderzoeksproces en de kwaliteit van de onderzoeksresultaten plaats.

5.1. Discussie

De GDPR is nieuwe wetgeving die vanaf 2018 van kracht is geworden en een beperkte *body of knowledge* kent: er zijn niet veel eerdere onderzoeken uitgevoerd naar de toepassing van de GDPR. Dit onderzoek draag bij aan de opbouw van de *body of knowled*ge omtrent deze wetgeving. Het kwalitatieve karakter van het onderzoek maakte het mogelijk om het onderwerp in de diepte te verkennen. Het gebruik van een gemengde kwantitatieve en kwalitatieve methode versterkt de interne validiteit en betrouwbaarheid van het onderzoek.

De bij dit onderzoek betrokken experts zijn geselecteerd op basis van kennis van de GDPR en kennis van de eigen organisatie, wat heeft geresulteerd in valide input in de interviews die echter wel sterk gericht was op de GDPR. Verbeteringen van het model zijn dus doorgevoerd op basis van inzichten vanuit de GDPR en niet vanuit EA of DM. De gekozen experts waren echter wel goed in staat om de onderzoeksvragen te beantwoorden. De ingevulde vragenlijsten zijn na het invullen doorlopen om fouten uit te sluiten.

De beperkte tijd die beschikbaar was voor het uitvoeren van het onderzoek (februari tot juli 2019) hebben het onderzoek beperkt tot twee iteraties. Dit betekent dat het model niet is doorontwikkeld tot de maximale tevredenheid, wat een mogelijke impact heeft op de interne validiteit van de uiteindelijke vragenlijst en het overeenkomstige AVG *maturity model*. Door het op afstand bevragen van twee van de vier experts is één van deze vragenlijsten bij de tweede iteratie foutief ingevuld. Hierdoor konden deze resultaten worden meegewogen, wat de uiteindelijke resultaten mogelijk heeft beïnvloed.

De interviews die gericht waren op verbetering van het model zijn afgenomen op basis van vooraf opgestelde vragen. Tijdens deze interviews zijn er elementen benoemd, waarvan sommige bij de evaluatiefase zijn teruggekomen, zoals het gebruik van PIA's en specifieke standaarden voor informatiebeveiliging. Het vasthouden aan de vooropgestelde methode heeft een bijdrage geleverd aan de betrouwbaarheid van het onderzoek. Publicatie van de interviews in de bijlage van dit rapport is echter niet mogelijk vanwege de vertrouwelijkheid van deze gegevens.

Beide caseorganisaties hadden uiteenlopende functies en verschillende grondslagen om persoonsgegevens te verwerken. Deze verzameldoelen waren breder dan bijvoorbeeld alleen het personeels- of klantenbestand. Eén van de organisaties had een belangrijke taak in het verzamelen van bijzondere persoonsgegevens (te weten geslacht en geaardheid), wat heeft bijgedragen aan de externe validiteit van het onderzoek. De caseorganisaties betreffen wel uitsluitend publieke organisaties binnen Nederland, waardoor de resultaten niet geëxtrapoleerd kunnen worden naar organisaties buiten Nederland of commerciële organisaties binnen Nederland, hetgeen invloed kan hebben op de externe validiteit van dit onderzoek.

De focus op Nederland is tevens van belang voor het afnemen van het model (vaststellen van de volwassenheid), omdat niet de GDPR-wetgeving zélf als fundament is gekozen, maar de Nederlandse vertaling: de uitvoeringswet of UAVG (Uitvoeringswet Algemene verordening gegevensbescherming, 2018). In de uitvoeringswet worden uitzonderingsgronden benoemd waar ruimte voor wordt gegeven in de GDPR. Een concreet voorbeeld is artikel 3 UAVG waarin de verwerking van

persoonsgegevens door de krijgsmacht is geregeld. De verwerking van persoonsgegevens door de krijgsmacht kan buiten de reikwijdte van de AVG worden geplaatst, waardoor de verwerking ook niet middels het *maturity model* kan worden getoetst. Daarnaast wordt het verzameldoel voor publieke organisaties vaak bepaald door een wettelijke taak. Deze verzamelingsgronden kunnen breed worden geformuleerd en geïnterpreteerd, waardoor een instantie meent veel gegevens te kunnen verzamelen en bewaren. Het *maturity model* kan niet nagaan of dit type beslissing dan wel de daarachter liggende redenering redelijk is.

5.2. Conclusie

Dit onderzoek is gericht op het ontwerp van een model om de volwassenheid op GDPR-gebied te kunnen meten, waarbij de centrale onderzoeksvraag als volgt is geformuleerd: *Hoe kan het volwassenheidsniveau van organisaties op het gebied van de GDPR worden gemeten, zodat het management en externe actoren in staat zijn om de mate van compliance objectief vast te stellen?*

Een *maturity model*, in dit geval voor de GDPR, maakt het mogelijk om de implementatie van wetgeving door een organisatie op objectieve wijze vast te stellen. Door een organisatie op basis van een *maturity model* te beoordelen, worden de prestaties binnen het meetgebied inzichtelijk gemaakt. Het onderhavige model werkt met een score van één tot en met zes. De score geeft de mate van volwassenheid per deelgebied aan. Om het model (objectief) vorm te geven is gebruikgemaakt van een vragenlijst. Er is gekozen voor gesloten vragen met korte antwoordopties en een volgordelijkheid (voorgeschreven volgorde van vragen). Het afnemen van deze vragenlijst resulteert in een scoring op het model. Deze scoring geeft de volwassenheid van een organisatie op één van de zes deelgebieden weer. Dit geeft inzicht in hoe de organisatie presteert op het deelgebied en hoe de organisatie zich op dat gebied kan doorontwikkelen. Deze scoring kan vervolgens inzichtelijk worden gemaakt aan diverse stakeholders en belanghebbenden binnen de organisatie.

Middels de Design Science Research-methode werd het model ontwikkeld in twee cycli van ‘bouwen’ en ‘evalueren’. Uit de disciplines van EA en DM zijn er bestaande en beproefde *maturity models* gekozen die de volwassenheid van organisaties binnen deze disciplines vaststellen. De GDPR is opgebouwd uit kernaspecten die verdeeld zijn over het opslaan en de verwerking van gegevens. Deze kernaspecten zijn vervolgens gekoppeld aan de EA en DM-onderdelen. Elementen uit de EA en DM-onderdelen zijn dus de input geweest voor het opgestelde GDPR *maturity model*. Middels de TAM-vragenlijst (Davis, 1989) is de verwachte bruikbaarheid (PU), het verwachte gebruiksgemak (PEOU) en de Intentie voor gebruik bevraagd (IU) op een zevenpunts-Likertschaal. Dit heeft geresulteerd in de scores van een 4.5 (PU), 5.7 (PEOU) en 5 (IU). Om het model door te ontwikkelen is respondenten gevraagd naar de relevantie van de inhoud van de vragenlijst. Evaluatie van de vragen heeft geresulteerd in het aanpassen van negen vragen. Verder is één vraag na de eerste iteratie verwijderd, omdat hieromtrent geen sprake was van algemene tevredenheid of consensus. Na de tweede iteratie was sprake van consensus of stabiliteit voor acht van de aangepaste vragen. Het model is in twee iteraties ontwikkeld, waarbij de algemene tevredenheid is toegenomen van 7 naar 7.5.

5.3. Implicaties voor de praktijk

Dit onderzoek heeft een bruikbaar GDPR *maturity model* (zie de vragenlijst en Tabel 6) opgeleverd. Het inzetten van dit model is met name van waarde als instrument om een nulmeting mee uit te

voeren en voortgang mee te meten. Voor de toepassing van het model is inhoudelijke kennis van de GDPR noodzakelijk. Het model is bruikbaar voor grote organisaties waarin diverse GDPR-rollen met bijbehorende expertise aanwezig zijn. Het *maturity model* biedt inzicht in de mate waarin de GDPR wordt toegepast en bied handelingsperspectief op organisatieniveau, maar niet op technisch niveau.

Het in kaart brengen van de volwassenheid door het afnemen van de vragenlijst maakt inzichtelijk waar de organisatie zich bevindt op het model en waar de organisatie maatregelen kan nemen. Door het nemen van deze maatregelen groeit de organisatie in volwassenheid en is zij beter is staat om de GDPR toe te passen. Hierdoor kan een organisatie gefaseerd groeien naar het gewenste eindstadium.

Voor kleine organisaties waarin geen kennis van EA, DM en de GDPR aanwezig is, leent dit model zich niet. Door het gebruik van terminologie en het hanteren van een hoog abstractieniveau (bijvoorbeeld de aanwezigheid van een strategie) is kennis van GDPR en een redelijke organisatieschaal vereist.

5.4. Aanbevelingen voor vervolgonderzoek

Het onderzoek beveelt een vijftal mogelijkheden voor verder wetenschappelijk onderzoek aan:

Aanbeveling 1: Betrek een grotere en meer diverse populatie bij het onderzoek
De huidige populatie van het onderzoek bestaat uit vier personen van twee organisaties. Deze personen zijn geselecteerd op basis van hun rol als expert binnen deze organisaties. Het betrekken van vier personen maakt de statistische basis van het onderzoek niet solide. Om het onderzoek meer interne validiteit te geven en sadistischer significanter te maken, dient het bij een grotere doelgroep te worden uitgevoerd.

Aanbeveling 2: Generaliseer de resultaten naar andere typen organisaties
Het onderzoek is uitgevoerd bij publieke organisaties binnen Nederland. Deze resultaten zijn niet verder te generaliseren naar andere typen non-profitorganisaties of commerciële organisaties.
Commerciële organisaties verwerven gegevens niet op basis van een nadrukkelijke wettelijke bevoegdheid, terwijl dit voor de onderzochte twee organisaties wel het geval was. Ook worden er voor commerciële organisaties in mindere mate bepaalde rollen voorgeschreven. Daarnaast hebben commerciële organisaties andere drijfveren dan non-profitorganisaties, waarbij de nadruk ligt op winstgevendheid, wat invloed kan hebben op de toepassing van de GDPR. Om dit onderzoek meer externe validiteit te geven, dient het ook bij commerciële organisaties binnen en buiten Nederland te worden uitgevoerd.

Aanbeveling 3: Voer het onderzoek uit bij een gegevensverwerker
Dit onderzoek is alleen uitgevoerd bij een verwerkingsverantwoordelijke (dat wil zeggen verantwoordelijk voor de verwerking van persoonsgegevens). Veel (kleinere) organisaties besteden de verwerking van persoonsgegevens echter uit aan een gegevensverwerker. Het uitvoeren van een soortgelijk onderzoek bij een gegevensverwerker biedt meer inzicht in de keten waarin persoonsgegevens vaak worden verwerkt, waarin ook verwerkers een belangrijke rol spelen.

Aanbeveling 4: Betrek een expertpopulatie die sterker betrokken is bij EA en DM
De huidige bij dit onderzoek betrokken experts zijn geselecteerd op basis van kennis van de eigen organisatie en de GDPR, en niet op basis van kennis van EA en DM, terwijl het model is opgesteld op basis van deze disciplines. Verbeteringen die deze experts hebben aangedragen zijn vrijwel uitsluitend gericht geweest op de GDPR, mogelijke verbeteringen op het gebied van EA en DM zijn niet doorgevoerd. Daarnaast hebben de aangedragen verbeteringen door de GDPR-experts een

verdringend effect gehad op elementen uit EA en DM, zoals de vragen gerelateerd aan datastrategie en kwaliteit.

Aanbeveling 5: *Gebruik het interview voor het vaststellen van het volwassenheidsniveau om het model te verbeteren*
Het eerste interview van dit onderzoek heeft plaatsgevonden om het model te toetsen op de betrokken organisaties. Hierbij zijn diverse termen en elementen uit de GDPR benoemd. Deze elementen zijn niet meegenomen in de verbetering van het model vanwege de vooropgestelde aanpak en de navolgbaarheid van het onderzoek. Het direct verbeteren van het onderzoek bij het toepassen van het model maakt snelle ontwikkeling in minder stappen mogelijk.

6. Bibliografie

Aiken, P. (2007). Measuring Data Management Practice Maturity: A Community's Self-Assessment. *Computer*, *40*(4), 42-50.

Becker, J., Knackstedt, R., & Poppelbus, J. (2009). Developing Maturity Models for IT Management – A Procedure Model and its Application. *Business & Information Systems Engineering, 1*(3), 213-222.

Blosch, M., & Burke, B. (2015). IT score Overview for Enterprise Architecture. Geraadpleegd van https://www.gartner.com/en/documents/3092223/itscore-overview-for-enterprise-architecture

Brous, P., Janssen, M., & Vilminko-Heikkinen, R. (2011). *Coordinating Decision-Making in Data Management Activities: A Systematic Review of Data Governance Principles.* Berlijn, Duitsland: Springer.

CMMI institute. (2014). *Data Management Maturity Model introduction.* Geraadpleegd van https://cdn.ymaws.com/www.globalaea.org/resource/collection/68814379-BF7E-41C8-B152-18A617F9C0AA/Data_Management_Maturity_Model_Introduction_-_Dec_12_2014.pdf

Curley, M. (2016). *IT Capability Maturity Framework* (2nd ed). 's-Hertogenbosch, Nederland: Van Haren.

DAMA. (2014). Data Management Capability Assessment Model. Enterprise Data Management Council.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly, 13*(3), 319-340.

Digitale overheid. (2017). CIP-overheid maakt AVG Privacy Suite. Geraadpleegd van https://www.digitaleoverheid.nl/nieuws/cip-overheid-maakt-grip-op-privacy-avg-compliant-grijpbaar-en-implementeerbaar/

Forrester. (2015). The Forrester Enterprise Architecture Maturity Assessment. Geraadpleegd van

https://www.forrester.com/report/The+Forrester+Enterprise+Architecture+Maturity+Assessment+Q2+2015/-/E-RES96181.

Freiherr, A., & Zeiter, A. (2018). Implementing the EU General Data Protection Regulation: A Business Perspective. Geraadpleegd van https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl2&div=92&id=&page=

Henderson, D. (2018). GDPR: It's All in the Data Management Controls, Ready or Not. Geraadpleegd van https://www.firstsanfranciscopartners.com/blog/gdpr-data-management-controls/

Hendrickson, A. R., Massey, P., Cronan, T. P. (1993). On the Test-Retest Reliability of Perceived Usefulness and Perceived Ease of Use Scales. *MIS Quarterly V17*, 227-230.

Hevner, A., March, S. T., Park, J., & Ram. S. (2004). Design Science in Information Systems Research. *MIS Quarterly, 28*(1), 75-105.

Lankhorst, M. (2009). *Enterprise Architecture at Work.* Ostfildern, Duitsland: Mairdumont.

Luftman, J. N. (2000). Assessing Business – IT alignment Maturity. *Communications of AIS,* 4(14), 1-14.

Meyer, H. O. (2011). *An Analysis of Enterprise Architecture Maturity*. Maynooth Ireland: Innovation Value Institute.

NASCIO. (2003). *NASCIO Enterprise Architecture Maturity Model.* Geraadpleegd van https://www.nascio.org/Portals/0/Publications/Documents/2003/NASCIO-EAMM.pdf.

Pandit, H. J., O'Sullivan, D., & Lewis, D. (2018). *Exploring GDPR Compliance Over ProvenanceGraphs Using SHACL.* Geraadpleegd van http://ceur-ws.org/Vol-2198/paper_120.pdf

Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (2008). *The Design Science Research Process: A model for producing and presenting information systems research*. Geraadpleegd van https://pdfs.semanticscholar.org/e1fa/ec8846289113fdeb840ff3f32d102e46fbff.pdf

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45-77.

PWC Nederland. (2017). *Privacy Governance onderzoek.* Geraadpleegd van https://www.pwc.nl/nl/assets/documents/pwc-privacy-governance-onderzoek-2017.pdf.

Ross, J. W. (2003). *Creating a strategic IT architecture competency: learning in stages.* Geraadpleegd van http://www.umsl.edu/~lacitym/misqearch.pdf

Saunders, M. N. (2015). *Research Methods for Business Students.* Boston, MA: Pearson.

Schermer, B. W., Hagenauw, D., & Falot, N. (2018). *Handleiding Algemene Verordening Gegevensbescherming en uitvoeringswet Algemene Verordening Gegevensbescherming.* Geraadpleegd van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggegevensbescherming.pdf:

Spruit, M., & Pietzka, S. (2014). MD3M: The master data management maturity model. *Computers in Human Behavior V51*.

Szajna, B. (1994). Software Evaluation and Choice: Predictive Validation of the Technology Acceptance Instrument. *MIS Quarterly*, *18*(3), 319-324.

De Bruin, M. R. & Rosemann, M (2007). *Using the Delphi Technique to Identify BPM Capability Areas.* Brisbane, Australia: AIS Electronic Library (AISeL).

The Office of Management and Budget. (2009). *OMB EA Assessment Framework 3.1.* Washington DC: The Office of Management and Budget (OMB).

The open group. (2018). TOGAF® Standard, Version 9.2. Geraadpleegd van http://pubs.opengroup.org/architecture/togaf9-doc/arch/

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Elsevier, 34(1), 134-153.

United States Department of Commerce. (2007). *Enterprise Architecture Capability.* United States Department of Commerce.

United States government accountability office. (2012). *GAO-10-846G Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management (Version 2.0).* Geraadpleegd van https://www.gao.gov/assets/80/77233.pdf

Vallerand, J., Lapalme, J., & Moïse, A. (2017). Analysing enterprise architecture maturity models: a learning perspective. *Enterprise Information Systems*, *11*(6), 859-883.

Van Looy, A., De Backer, M., Poels, G., & Snoeck, M. (2013). Choosing the right business process maturity model. *Information & Management*, *50*(7), 466-488.

Wendler. (2012). The maturity of maturity model research: A systematic mapping study. *Information and Software Technology, 54*(12), 1317-1339.

Yin, R. K. (2003). *Case study research design and methods.* Thousand Oaks, CA: Sage.

Bijlage

Bijlage 1 TOGAF principes

Principe	**Beschrijving**
Begrijpbaar	De onderliggende principes kunnen snel worden begrepen door individuen in de hele organisatie. De bedoeling van het principe is duidelijk en ondubbelzinnig, zodat overtredingen, al dan niet opzettelijk, worden geminimaliseerd
Robuust	Maakt beslissingen van goede kwaliteit mogelijk over architecturen en plannen. Elk principe moet voldoende definitief en nauwkeurig zijn om consistente besluitvorming in complexe, mogelijk controversiële situaties te ondersteunen.
Compleet	Elk mogelijk principe over het beheer van informatie en technologie, is gedefinieerd voor de organisatie. De principes hebben betrekking op elke waargenomen situatie.
Consistent	Strikte naleving van één principe kan een losse interpretatie van een ander principe vereisen. De set van principes moet op een manier worden uitgedrukt die een evenwicht tussen de interpretaties mogelijk maakt. Principes mogen niet in tegenspraak zijn met elkaar.
Stabiel	Principes moeten blijvend zijn, maar toch aanpasbaar aan eventuele veranderingen. Er dient een wijzigingsprocedure te worden opgesteld voor het toevoegen, verwijderen of wijzigen van beginselen nadat deze in eerste instantie zijn geratificeerd

Bijlage 2 DM principes

Principe	Beschrijving
Organisatie	De organisatie bepaald de doelen voor de datahuishouding en stelt de kwaliteitsstandaarden voor data vast. Rollen, besluiten, domeinen, taken en verantwoordelijkheden met betrekking tot de verwerking van data zijn vastgelegd.
Alignment	Data heeft als doel om waarde voor de organisatie te creëren, de verwerking van data is dus geen doel op zich. *Data governance* moet er voor zorgen dat data bruikbaar is voor relevante stakeholders binnen de organisatie.
Compliance	Binnen een organisatie is er een autoriteit voor de handhaving van beleid en procedures. Het beleid wordt bepaald in samenspraak tussen *Business* en IT, zodat het binnen de gehele organisatie toepasbaar is. Middels *governance* wordt verantwoording van dit beleid geïmplementeerd.
Common understanding	Een *enterprise data model* borgt een zelfde interpretatie van data door de standaardisatie van metadata. Dit is belangrijk voor de bruikbaarheid en traceerbaarheid van gegevens.

Bijlage 3 Analyse EA artikelen

Paper	Titel	Referentie	Engels	Maturity models	Literature review	volledige tekst beschikbaar
1.	Analysis of enterprise architecture maturity models	Fernandez et al., 2017	0	0		
2.	Analysing enterprise architecture maturity models: a learning perspective	Vallerand et al., 2017	X	X	X	X
3.	Enterprise Architecture A maturity model based on TOGAF ADM	Proenca & Bordinha, 2017	X	X	0	
4.	Validation architecture for information technology management in smart cities	Gongora & Bernal ., 2016	0			
5.	Methods and techniques for maturity assessment	Proenca, 2016	X	X	0	
6.	Approach to evaluation of maturity level in enterprise Architecture	Martinez et al ., 2015	0			
7.	Enterprise architecture of Colombian higher education	Llamosa-villabla et al ., 2015	X	0		
8.	Specifics of project in the area of enterprise architecture development	Koznov et al ., 2015	X	X	0	
9.	An architecture framework for enterprise	Franke et al ., 2014	X	X		

	IT service availability analysis					
10.	Towards a framework for enterprise architecture analytics	Schmidt et al ., 2014	X	X	0	
11.	Case study on enterprise architecture management based on TOGAF	Gao & Chen, 2012	X	X	0	
12.	Architecting Business and IS/IT stractegic alignment for extended enterprises	Cuenca et al ., 2014	X	X	0	
13.	An analysis of enterprise architecture maturity frameworks	Meyer et al ., 20111	X	X	X	X
14.	Enterprise architecture framework with early business/ICT alignment for extended enterprises	Cuenca et al ., 2010	X	X	0	
15.	The dynamic architecture maturity matrix: Instrument analysis and refinement	Van Steenbergen et al ., 2010	X	X	0	

Bijlage 4 Analyse DM artikelen

Paper	Titel	Referentie	Engels	Maturity models	link met DM	volledige tekst beschikbaar
1.	MD3M: The master data management maturity model	M Spruit, K Pietzka 2015	x	x	x	x
2.	Developments in Research Data Management in Academic Libraries: Towards an Understanding of Research Data Service Maturity	Cox, Andrew M.; Kennan, Mary Anne; Lyon, Liz; et al., 2017	x	0	x	x
3.	MAMD 2.0: Environment for data quality processes implantation based on ISO 8000-6X and ISO/IEC 33000	Carretero, Ana G.; Gualo, Fernando; Caballero, Ismael; et al. 2017	x	0	x	x
4.	Mind the gap - Assessing maturity of demand planning, a cornerstone of S&OP	Vereecke, Ann; Vanderheyden, Karlien; Baecke, Philippe; et al. 2018	x	0	0	x
5.	Maturity assessment of HRM processes based on HR process survey tool: a case study	Zare, Milad Shams; Tahmasebi, Reza; Yazdani, Hamidreza 2018	x	0	0	x

Bijlage 5 Overzicht backward snowballing EA maturity frameworks

Naam model	**referentie**
Gartner's ITScore for EA	Blosch en Burke (2015).
Forrester's EA maturity assessment tool	Frorrester (2015).
IVI IT-Capability Maturity Framework	Curley (2016);
NASCIO Enterprise Architecture Maturity Model	NASCIO (2003).
SEI Capability Maturity Model Integration	Curley (2016).
USDoC Enterprise Architecture Capability Maturity Model	United States Department of Commerce (2007).
USGAO Enterprise Architecture Management Maturity Framework	United States Government Accountabilit Office (2012).
USOMB Enterprise Architecture Assessment Framework	Office of Management and Budget (2009).
COBIT/ValIT	
Luftmann's SAMM	Luftman (2000).
The MIT Center for Information Systems Research Enterprise Architecture Maturity Model	Ross (2003).

Bijlage 6 GOA maturity levels

Stage		Beschrijving
0	Creëren van EA awareness	Geen plannen voor EA of de toepassing van EA binnen de organisatie. EA ontbreekt.
1	Creëren van EA instituties en commitment	Architecten hebben positie binnen de organisatie , EA wordt ontwikkeld.
2	Creëren van het managementfundament voor EA	EA programma ingericht, bestuurlijke inbedding van EA is geborgd.
3	Initiële EA versies ontwikkelen	Betrokken stakeholders en huidige en toekomstige situatie in kaart gebracht
4	Opleveren en gebruiken van EA om resultaten te leveren	Plan voor transitie van huidige naar toekomstige situatie
5	Door ontwikkelen van EA voor organisatie transformatie	Integratie tussen verschillende EA producten, toetsing van producten door ander partijen
6	Continu verbeteren van EA om organisatie optimalisatie te bereiken	Alle 59 elementen (stage 0-5) zijn positief beoordeeld.

Bijlage 7 GOA & GDPR relatie

Attribuut	Relatie GDPR	Motivatie
EA management actie vertegenwoordiging		
1. Demonstratie van commitment	Rechtmatigheid, behoorlijkheid, transparantie	Beschrijving van beleid (voor EA) waarbij een verantwoordelijke is aangewezen. Dit maakt het mogelijk om een verantwoordelijke voor gegevens binnen een organisatie aan te wijzen. Dit is tevens toepasbaar op de verwerking van persoonsgegevens
2. Voorzien in middelen om commitment te bereiken	Rechtmatigheid, behoorlijkheid, transparantie.	Binnen de organisatie zijn middelen aanwezig om de inzet van EA meetbaar maken en te realiseren. Dit is te relateren aan de verwerking van gegevens en het toekennen van middelen om deze verwerking van mogelijk te maken.
3. Demonstreren van commitment	Geen	
4. Verificatie van commitment	Geen	
Functionele EA vertegenwoordiging		
1. Governance	Rechtmatigheid, behoorlijkheid, transparantie.	Voldoende middelen om EA doelen te bereiken, verantwoordelijke aangewezen. governace over EA ingericht. Tevens toepasbaar voor verwerking van gegevens.
2. Content	Geen	
3. Gebruik	Minimale gegevensverwerking	Gebruik van EA is beschreven, dit is ook toepasbaar op de eigen op de eigen GDPR policy binnen organisatie.
4. Meetbaarheid	Geen	
Vertegenwoordiging kern elementen		
1. Compleetheid	Juistheid	Gebruik van standaarden voor ontwikkeling van EA, om de juistheid van verwerking van gegevens te borgen zijn standaarden op dit gebied ook toepasbaar.
2. Gebruik	Doelbinding	Bewustwording van EA binnen de organisatie is aanwezig, dit is ook toepasbaar op de verwerking van persoonsgegevens.
3. Resultaten	Rechtmatigheid, behoorlijkheid, transparantie	Er is externe controle op de eigen EA. Deze toetsingsvorm kan ook worden toegepast op de verwerking van persoonsgegevens conform GDPR.
EA als enabler		
1. Leiderschap	Geen	
2. Personeel	Geen	
3. Processen	Rechtmatigheid, behoorlijkheid, transparantie	Doel van EA is duidelijk omgeschreven, door ontwikkeling ingericht en gecommuniceerd. Deze uitgangspunten zijn ook toepasbaar op de GDPR.
4. Tools	Geen	

Bijlage 8 OMB & GDPR relatie

Deelgebied	Relatie GDPR	Motivatie
Compleetheid		
Doel EA en transitie plan	Geen	
Architectuur prioriteiten	Geen	
Scope en compleetheid	Geen	
Gebruik van internet protocol version 6 (IPv6)	Geen	
Gebruik		
Integratie transitie en verbeter planning	Geen	
CPIC integrate	Geen	
FEA referentie model	Geen	
Samenwerking en hergebruik (applicaties)	Minimale gegevensverwerking	OMB is gericht op hergebruik van functionaliteiten. Kan worden toegepast op persoonsgegevens, enkelvoudige opslag van deze gegevens.
EA governance, programma management, verandermanagement	Geen	
Resultaten		
Gebruik van EA performance verbetering	Geen	
Kosten besparing en kosten vermijding	Geen	
Kwaliteit IT infrastructuur kwaliteit	Geen	
Meten van EA waarden	Geen	

Bijlage 9 MD3M *maturity levels*

Niveau	**Beschrijving**
1: Initial	Sprake van eerste bewustzijn
2: Repeatable	Maatregelen van individuen worden uitgevoerd, geen verbinding met projecten.
3: Defined process	Eerste samenwerking op tactisch niveau. Bewustzijn wordt gecreëerd voor het bestaan van andere initiatieven.
4: Managed and measurable	Er zijn best practices voor het omgaan met MDM. Er zijn gedefinieerde processen op tactisch niveau
5: Optimized	Geoptimaliseerde gebruik MDM, de efficiëntie van de organisatie is verbeterd.

Bijlage 10 MD3M & GDPR relatie

MD3M-basisbeginselen	Relatie GDPR	Motivatie
Data Model		
Definition of Master Data	Geen	
Master Data Model	Rechtmatigheid, behoorlijkheid en transparantie	Gericht op inzicht in Masterdata, kan tevens worden toegepast op verwerking persoonsgegevens. Transparantie en inzicht zijn tevens van groot belang bij de verwerking van persoonsgegevens.
Data Landscape	Rechtmatigheid, behoorlijkheid en transparantie	Beschrijft het inzicht van een bedrijf in de verwerking van data. Het inzicht is ook toepasbaar voor wie in wie en welke bedrijfsonderdelen er toegang hebben tot welke persoonsgegevens
Data Quality		
Assessment of Data Quality	Juistheid	Het hebben van juiste gegevens, van voldoende kwaliteit is ook toepasbaar op persoonsgegevens Zo dient er toetsing van de juistheid van deze gegevens plaats te vinden.
Impact on Business	Geen	
Awareness of Quality Gaps	Juistheid	Het hebben van juiste gegevens is ook bij persoonsgegevens van belang, medewerker dienen zich bewust te zijn van de gevolgen van de verwerking van onjuiste gegevens
Improvement	Juistheid	Om bij te dragen aan de juistheid van (persoons) gegevens worden initiatieven ontplooid.
Usage & Ownership		
Data Usage	Rechtmatigheid, behoorlijkheid en transparantie Minimale gegevensverwerking	Inzicht in wie en welke bedrijfsonderdelen er toegang hebben tot welke persoonsgegevens en wie deze kunnen bewerken. Dit draagt bij aan transparantie en rechtmatige verwerking (geen ongeoorloofd toegang tot gegevens
Data Ownership	Rechtmatigheid, behoorlijkheid en transparantie	Eigenaarschap van gegevens is centraal belegd (IPV per bedrijfsonderdeel) dit draagt bij aan transparantie in inzicht van de verwerking.
Data Access	Rechtmatigheid, behoorlijkheid en transparantie Minimale gegevensverwerking	Er zijn geautomatiseerde processen om toegang te krijgen tot de eigen persoonsgegevens, er kan ter stond toegang worden verleend
Data Protection		
Data Protection	Integriteit en vertrouwelijkheid	Toegang tot persoonsgegevens wordt op basis van rollen verstrekt, er is beveiligingsbeleid voor de toegang tot persoonsgegevens. Dit draagt bij aan een afdoende beveiliging van de gegevens.

Maintenance		
Storage	Opslagbeperking	Opslag is logisch, er vindt regelmatig controle plaats op dubbelingen in gegevens, hierdoor wordt overmatige opslag beperkt.
Data Lifecycle	Opslagbeperking	Er is aandacht voor data lifecycle management, waardoor gegevens tijdig vernietigd worden.

Bijlage 11 DCAM & GDPR relatie

DCAM kern component	Levels	Relatie GDPR	Motivatie
DATA MANAGEMENT STRATEGY De DM management strategie bepaald hoe data de DM organisatie & governance is ingericht en gefinancierd. Er is een lange termijn visie en kritische stakeholders zijn aligend.	1-7	Doelbinding	De principes van vastlegging (waarom worden persoonsgegevens opgeslagen) en mapping kunnen op doelbinding worden toegepast.
THE DATA MANAGEMENT BUSINESS CASE AND FUNDING MODEL Het DM business case en financieringsmodel creëren financiering voor DM programma's.	1-3	Geen	
DATA MANAGEMENT PROGRAM DM pogramma is een organisatorische functie gewijd aan het beheer van gegevens.	1-5	Geen	
DATA GOVERNANCE Data Governance is de ruggengraat van een succesvol Data Management-programma. Data Governance is het proces van het vaststellen van normen, het definiëren van regels, het vaststellen van beleid en implementeren overzicht om te zorgen naleving van best practices voor gegevensbeheer.	1-7	Rechtmatigheid, behoorlijkheid en transparantie	Eigenaarschap voor gegevens is belegd en wordt gecommuniceerd. Er is inzichtelijk wie op basis waarvan toegang tot welke gegeven heeft.
DATA ARCHITECTURE Ontwerpt , beheer en controle van Data. Data-architectuur identificeert datadomeinen, metadata, definieert kritieke gegevenselementen, bepaalt taxonomieën en anthologieën. Cruciaal om te verzekeren dat de betekenis van data is nauwkeurig en ondubbelzinnig is en het gebruik van gegevens consistent en transparant is.	1-3	Integriteit en vertrouwelijkheid Opslagbeperking	Er is sprake van een data architectuur die de kwaliteit van gegevens bewaakt en een minimale opslag borgt
TECHNOLOGY ARCHITECTURE Technology Architecture verwijst naar de strategie, het ontwerp en de implementatie	1-4	Integriteit en vertrouwelijkheid	Fysieke infrastructuur is voldoende beveiligd en onderhouden. Dit maakt veilige en integere opslag en verwerking van gegevens mogelijk.

van de fysieke architectuur in ondersteuning van de gedefinieerde gegevens architectuur.			
DATA QUALITY Data quality omvat het "wat/wie/wat/hoe van de gegevenskwaliteit.	1-3	Juistheid	Rollen voor data kwaliteit belegd. Strategie aanwezig.
DATA OPERATIONS PROGRAM Data operions programs kunnen centraal of gefedereerd in een organisatie werken. In elk van beide modellen moet Data Operations afgestemd zijn op de organisatie, capaciteiten en strategie voor bedrijfsgegevensbeheer	1-2	Geen	

Bijlage 12 DMM maturity levels

Niveau	Beschrijving
1. Performed	Processen zijn ad-hoc, reactief en worden niet toegepast over verschillende domeinen.
2. Managed	Processen worden gepland en uitgevoerd conform beleid door getrainde werknemers in samenspraak met relevante stakeholders
3. Defined	Een set van standaard processen is vastgelegd en wordt gevolgd. Specifieke behoeftes worden vervuld door processen conform beleid te baseren op de standaard processen,
4. Measured	Criteria voor processen zijn vastgelegd en worden gebruikt voor data management. Dit houdt in: management van afwijkingen, voorspellingen en analyse. Processen worden gemanaged tijdens de uitvoering.
5. Optimized	Processen worden geoptimaliseerd door het toepassen van niveau 4 analyse voor verbetermogelijkheden. Best practices worden gedeeld met andere bedrijven.

Bijlage 13 DMM & GDPR relatie

DMM Domein	Relatie GDPR	Motivatie
Data management Strategy Data Management Strategy, Communications, Data Management Function, Business Case Funding	Doelbinding	Datadoelen en organisatiedoelen zijn verbonden. Er is een duidelijke motivatie om data te verzamelen
Data Governance Governance Management, Business Glossary, Metadata Management	Rechtmatigheid, behoorlijkheid en transparantie	Best practices voor sturing op data en breed draagvlak in de praktijk, CxO toezicht in de effectiviteit van data management
Data Quality Data Quality Strategy, Data Profiling, Data Quality Assessment, Data Cleansing	Juistheid	Best practices voor het definiëren van een aanpak voor het detecteren en corrigeren van foute data om te borgen dat de juiste data beschikbaar is voor gebruik in bedrijfsprocessen, beslissingen en planning. Dit borgt de juistheid van gegevens
Data Operations Data Requirements Definition, Data Lifecycle Management, Provider Management	Juistheid	Standaarden en eisen voor data en het managen van geïmplementeerde deze standaarden door de organisatie. Dit borgt de juistheid van gegevens.
Platform & Architecture Architectural Approach, Architectural Standards, Data Management Platform, Data Integration, Historical Data & Archiving	Integriteit en vertrouwelijkheid	Methoden en standaarden die borgen dat het datamanagementplatform de bedrijfsdata integreert, vasthoudt en archiveert om bedrijfsdoelen te ondersteunen.
Supporting Processes Measurement and Analysis, Process Management, Process Quality Assurance, Risk Management, Configuration Management	Integriteit en vertrouwelijkheid	opgestelde bedrijfsprocessen voor het beoordelen en implementeren, datamanagement in alle proces ingericht.

Bijlage 14 Overzicht integratie GDPR kernaspecten en maturity models EA en DM

Niveau	*GOA 2.0/ OMB 3.1 (EA)*	*MD3M (DM)*	*DCAM (DM)*	*DMM (DM)*	*afgeleide GDPR statement*
Integriteit en vertrouwelijkheid					
0	Geen	*	*	*	Aandacht voor integriteit en vertrouwelijkheid van persoonsgegevens is afwezig
1	Geen	Aan technische eisen voor beveiliging is voldaan	*	Standaarden voor implementatie van nieuwe data oplossingen, tenminste data management voor projecten	Aan technische eisen de beveiliging van persoonsgegevens is voldaan. Nieuwe oplossingen die persoonsgegevens verwerken worden getoetst aan deze standaarden
2	Geen	toegang tot data moet worden geactiveerd	Er is een data platform strategie	Data architectuur afgestemd met datamanagement strategie	Er wordt gelogd wie toegang heeft tot persoonsgegevens, er is een datamanagement strategie
3	Geen	rules voor toegang van rollen tot data	Tools voor data technologie worden doorontwikkeld en gestuurd	Data rationalisatie, implementatie van de data architectuur over de organisatie	Toegang tot persoonsgegevens wordt op basis van rules verstrekt. Er is aandacht voor rationalisatie van persoonsgegevens
4	Geen	paswoorden voor toegang voldoen aan beveiligingseisen	Data Storage Management strategie gedefinieerd en gestuurd	statische analyse van de data architectuur en verbeteringen op basis van deze analyse. Procesprestaties worden kwantitatief gemeten	Beveiligingsbeleid berust op standaarden, er een datamanagement strategie, Er is bewustzijn onder medewerkers voor informatiebeveiliging,
5	Geen	bewust onder medewerkers voor data beveiliging	It operationele risco planning in place	Delen van lessen van datamanagement. Bedrijfsprestaties worden kwantitatief gemanaged	Er is constant aandacht voor beveiliging van gegevens en lessen worden gedeeld

6	Geen	*	*	*	Vervalt

Niveau	*GOA 2.0/ OMB 3.1 (EA)*	*MD3M (DM)*	*DCAM (DM)*	*DMM (DM)*	*afgeleide GDPR statement*
Opslagbeperking					
0	*	*	*	Geen	Aandacht voor opslagbeperking van persoonsgegevens is afwezig
1	Geen	data is logisch opgeslagen, organisatie bekend met lifecycle management	*	Geen	Data is logisch opgeslagen, de organisatie is bekend met datalifecycle management
2	Geen	data opslag wordt regelmatig gecontroleerd, data wordt gezien als organisatie asset	Er zijn logische data domeinen	Geen	Opgeslagen persoonsgegevens worden gecontroleerd. Data is logisch opgedeeld in domeinen.
3	Geen	data opslag controle wordt automatisch uitgevoerd, handleiding voor lifecycle management van data	Taxonomie en ontologie en metadata model zijn in place	Geen	Er is regelmatig controle op de noodzaak van het opslaan van persoonsgegevens.
4	Geen	data base logica wordt regelmatig gecontroleerd op performance en logica, sprake van singel source of truth voor data	Data governace is ingericht	Geen	Er is sprake van één singel source of truth voor persoonsgegeven. Persoonsgegevens worden enkelvoudig opgeslagen.
5	Geen	data wordt op innovatie wijze opgeslagen, logging van wijzigingen in data	*	Geen	Persoonsgegevens zijn op innovatieve wijze opgeslagen, er is logging op door wie deze gegevens worden geraadpleegd
6	Geen	*	*	Geen	Vervalt

Niveau	*GOA 2.0 (EA)*	*OMB 3.1 (EA)*	*MD3M (DM)*	*DCAM (DM)*	*DMM (DM)*	*afgeleide GDPR statement*
Juistheid						
0	*	Geen	*	*	*	Aandacht voor juistheid van persoonsgegevens is afwezig
1	*	Geen	gevoel over juistheid van data, team bewust van redenen voor slechte kwaliteit, ondermaats kwaliteit bekend	*	Er zijn standaarden voor datakwaliteit en dataeisen	Er is binnen de organisatie bewustzijn voor de juistheid van gegevens, er zijn standaarden voor datakwaliteit
2	EA segmenten en federaties zijn in kaart gebracht en geprioriteerd	Geen	begrip gedefinieerd voor data kwaliteit, plaatsen van slechte kwaliteit bekend, belang van kwaliteit bekend	Er is een data kwaliteit programma, rollen zijn toebedeeld	Er is een strategie voor datakwaliteit, afgestemd met organisatiedoelen	Er is binnen de organisatie een begrip voor juistheid van gegevens. Er is een strategie voor datakwaliteit
3	ist en soll voor EA zijn beschreven, controle van producten aan framework	Geen	Begrip voor datakwaliteit is afgestemd met stakeholders, patronen worden onderzocht, benchmarking kwaliteit	De datakwaliteit wordt beoordeeld en doorontwikkeld	strategie voor datakwaliteit wordt opgevolgd, governace belegd	De juistheid van persoonsgegevens wordt getoetst. Er wordt invulling gegevens aan de strategie voor datakwaliteit
4	Transitieplan voor EA is aanwezig	Geen	Datakwaliteit wordt gemeten, bekend met gevolgen, verbeter maatregelen genomen	Data kwaliteitsplan is operationeel	Er vindt rapportage en controle plaats op datakwaliteit en er vindt aanpassing van de strategie plaats op basis van de meet uitkomsten	De juistheid van gegevens getoetst en uit de uitkomsten wordt opvolging gegeven. Datakwaliteit wordt gemeten en hier wordt over gerapporteerd

5	Integrale EA aanwezig	Geen	periodieke controle op data kwaliteit, zwakke plekken in data kwaliteit bekend, zelf assessment	*	Continue verbetering van datakwaliteit en vergelijking met externe partijen	Juistheid van gegevens wordt vergeleken met andere partijen, er is sprake van continue doorontwikkeling
6	EA wordt continu door ontwikkeld	Geen	*	*	*	Vervalt

Niveau	*GOA 2.0 (EA)*	*OMB 3.1 (EA)*	*MD3M (DM)*	*DCAM (DM)*	*DMM (DM)*	*afgeleide GDPR statement*
rechtmatigheid, behoorlijkheid, transparantie						
0	*	*	*	Er is een Data management office en deze heeft een eigenaar	*	Aandacht voor rechtmatigheid, behoorlijkheid, transparantie is afwezig
1	beschreven beleid, eigenaar voor EA aangewezen, training in EA, EA doel beschreven	geen	MD, Model aanwezig, zicht op gebruik, afdelen data individuele eigenaar, proces voor toegang tot data beschreven	Er zijn standaarden voor data management en deze zijn vastgesteld en gedeeld	Eigenaarschap van data is vastgelegd, functies zijn voor projecten ingericht	Eigenaarschap voor gegevens is vastgelegd, er is zicht op wie welke gegevens gebruikt
2	Budget beschikbaar, EA programma's aanwezig, tools aanwezig, meting van programma's	geen	zicht op masterdata per afdeling, zicht op toegang, rollen afdelen eigenaar gebruik en noodzaak zijn gedefinieerd, geen toegang tot data voor onbevoegde	Er zijn controles voor projecten opgesteld en er worden audits uitgevoerd	Er is sprake van een datagovernace structuur, rollen zijn belegd	Eigenaarschap voor gegevens is vastgelegd, en dit wordt gecommuniceerd. Er is sprake van datagovernace.
3	CXO betrokken bij EA, Middelen voor EA toebedeeld , EA voorgang wordt gemeten en gerapporteerd	geen	relaties en gebruik van masterdata zichtbaar, opslag en gebruik gemanaged eigenaarschap wordt helder gecommuniceerd, alle noodzakelijk data toegankelijk	Er is programma governace ingericht	Er een is organisatie brede datagovernace en deze is gedragen	Datagovernace is organisatie breed ingericht, persoonsgegevens zijn alleen toegankelijk wanneer strikt noodzakelijk
4	Goed gekeurde EA, voldoende personeel voor EA, meting en rapportage van EA producten en resultaten	geen	gebruik van masterdata door organisatie, geen overmatig gebruik, overzicht van al het data gebruik, data stewards zijn aangesteld, alleen toegang tot strikt noodzakelijk	Content governace is ingericht	Effecten van datagovernace worden kwantitatief gemeten & en aangepast op basis van deze resultaten	Er is zicht op al het datagebruik binnen de organisatie, dit gebruik wordt gecommuniceerd

5	Goedgekeurd en curerend EA, EA methodologie en tools worden gebruikt, onafhankelijke beoordeling van EA	geen	onderhoud van masterdata model, constant overzicht van data flows, data stewardship is promoted, alle medewerkers	Technologie governance is ingericht	Proces wordt continu verbeterd en vergeleken met externe partijen	Datagovernace is organisatie breed ingericht en wordt continu verbeterd
6	EA wordt gebruikt informeren van organisatie, EA tools en methodologie wordt continu verbeterd, externe assessment van EA	*	*	Data governace is over de organisatie heen ingericht	*	Vervalt

Niveau	*GOA 2.0 (EA)*	*OMB 3.1 (EA)*	*MD3M (DM)*	*DCAM (DM)*	*DMM (DM)*	*afgeleide GDPR statement*
Doelbinding						
0	*	*	*	Er is een Data management strategie (DMS) , afgestemd met stakeholders (business, technologie en operaties), er worden audits uitgevoerd	*	Aandacht voor doelbinding is afwezig
1	beleid voor EA is beschreven, EA rollen zijn benoemend	geen	begrip masterdata bekend, inzicht in impact data kwaliteit,	bedrijfseisen zijn verwerkt in de DMS strategie	Doel van datamangement is afgestemd met organisatie doel	Er is een basis defenitie voor doelbinding binnen de organisatie
2	EA board en programma's zijn aanwezig	geen	basis definities voor masterdata, onderwerp van gesprek, inzicht in specifieke impact	DMS definieert prioriteert en autoriseert het gebruik van data	Scope en doel voor datamangement gedefinieerd en goedgekeurd	Er is een datamagnement strategie waar doelbinding wordt geadresseerd
3	CXO is betrokken bij EA	geen	overstemming over Master data over afdelingen, financiële impact bekend	De DMS is aligned met IT architectuur en operaties, de DMS is gekoppeld aan busisness drivers	Scope van strategie is organisatie breed opgesteld en gedragen	Inzicht voor welke doelen persoonsgegevens over de organisatie heen worden verzameld en welke data wordt verzameld
4	EA wordt vastgesteld door CXO	geen	officiële definitie over master data, impact breder dan fin bekend, financiële argumenten van impact bekend	De DMS is verankerd is een governace structuur	Voortgang van datamangement strategie wordt gemeten en geëvalueerd	Persoonsgegevens die niet aan een doel te koppelen zijn worden actief verwijderd.

5	EA wordt door de organisatie heen gebruikt	geen	Interfaces om master data uit t te wisselen, formats aanwezig	De DMS bepaald wordt gebruikt om de voortgang van programma's wordt gemeten	Beste practices worden geselecteerd en geïmplementeerd	Doelbinding van persoonsgegevens wordt continu doorontwikkeld
6	EA wordt door CXO gebruikt voor planning, beleid en communicatie	*	*	De DMS is door vertaald naar trainingen	*	Vervalt

Niveau	*GOA 2.0 (EA)*	*OMB 3.1 (EA)*	*MD3M (DM)*	*DCAM / DMM (DM)*	*afgeleide GDPR statement*
Minimale gegevensverwerking					
0	*	*	*	Geen	Aandacht voor minimale gegevensverwerking is afwezig
1	*	standaarden voor interoperabiliteit van data aanwezig	bekend wie welke data kan gebruiken	Geen	Er is een definitie voor minimale gegevensverwerking
2	*	Compliance met standaarden voor interoperabiliteit	bekend of data ook daadwerkelijk worden gebruikt	Geen	Er is bekend wie welke gegeven binnen een organisatie kunnen verwerken
3	Vergelijkingsmechanisme en tools beschikbaar voor vergelijking huidige staat met beleid	hergebruik SRM service componenten, infrastructuur en informatie	toegang tot het noodzakelijke	Geen	Er is bekend of persoonsgegevens worden (rechtmatig) worden gebruikt
4	EA is geïntegreerd in andere disciplines	Hergebruik van SRM service componenten binnen de organisatie	Databases worden onderhouden	Geen	Persoonsgegevens die niet worden verwerkt worden verwijderd
5	*	Delen van SRM met andere organisaties	toegang kan snel worden verleend	Geen	Minimale gegevensverwerking wordt continu doorontwikkeld
6	EA wordt door CXO gebruikt voor informeren organisatie	*	*	Geen	Vervalt

Bijlage 15 Scoringsvragenlijst maturity model

Integriteit en vertrouwelijkheid

nummer	Vraag
1.	**Integriteit**: De mate waarin de gegevens in overeenstemming zijn met het afgebeelde deel van de realiteit, waarbij niets ten onrechte is toegevoegd, verdwenen of achtergehouden. **Vertrouwelijkheid**: Vertrouwelijkheid is een kwaliteitskenmerk van gegevens. Met vertrouwelijkheid wordt bedoeld dat een gegeven alleen te benaderen is door iemand die gemachtigd is het gegeven te benaderen. Wie gemachtigd is een gegeven te benaderen, wordt vastgesteld door de eigenaar van het gegeven. Is er binnen de organisatie aandacht voor de Integriteit en vertrouwelijkheid van persoonsgegevens?
	Nee: niveau 0 Ja: naar vraag 2
2.	Zijn er binnen uw organisatie standaarden gericht op integriteit en vertrouwelijkheid voor implementatie van nieuwe dataoplossingen, en zo ja welke zijn dit?
	Nee: niveau 1 Ja: zo ja welke? Door naar vraag 3
3.	Is er logging van het raadplegen of muteren van gegevens binnen de organisatie ingericht?
	Nee: niveau 2 Ja: op welke wijze Door naar vraag 4
4.	Wordt toegang tot persoonsgegevens op basis van rollen verstrekt?
	Nee: niveau 3 Ja door naar vraag 5
5.	Zijn medewerkers zich bewust van informatiebeveiliging, wat voor maatregelen zijn er door de organisatie genomen om dit bewustzijn te borgen?
	Nee: niveau 4 Ja maar geen maatregelen: niveau 5 Ja door naar vraag 6
6.	Hoe wordt er door de organisatie geleerd op het gebied van informatiebeveiliging en hoe worden deze lessen gedeeld?
	Delen van lessen en intern lerend vermogen: niveau 6
Niveau:	

Opslagbeperking

nummer	Vraag
1.	Zijn er beperkingen binnen de organisatie voor de opslag van persoonsgegevens?
	Nee: niveau 0 Ja: naar vraag 2

2.	**Datalifecycle**: De levenscyclus van gegevens biedt een hoog niveauoverzicht van de stadia die betrokken zijn bij succesvol beheer en behoud van gegevens voor gebruik en hergebruik van gegevens. • Data Capture • Data Maintenance • (optioneel) Data synthese, data samenbrengen • Data use • Data publication • Data Archiving • Data Purging (vernietiging) Is datalifecycle management ingericht?
	Nee: niveau 1 Ja: naar vraag 3
3.	Datadomeinen Op delen van data in verschillende groepen, b.v. klantdata, sensordata medewerkersdata. Welke datadomeinen worden er onderscheiden binnen de organisatie?
	Nee: niveau 2 Ja: naar vraag 4
4.	Wordt de opslag van persoonsgegevens op relevantie gecontroleerd?
	Nee: niveau 3 Ja: naar vraag 5
5.	Is er sprake van enkelvoudige opslag van gegevens?
	Nee: niveau 4 Ja: naar vraag 6
6.	Is er een proces voor het wijzigingen van persoonsgegevens ingericht?
	Nee: niveau 5 Ja: niveau 6
Score	

Juistheid

nummer	Vraag
1.	Zijn er standaarden of eisen voor de juistheid van gegevens binnen uw organisatie?
	Nee: niveau 0 Ja: naar vraag 2
2.	Zijn medewerkers zich bewust van deze standaarden?
	Nee: niveau 1 Ja: naar vraag 3
3.	**Datakwaliteit:** is de mate waarin data geschikt is voor het doel waarvoor ze gebruikt wordt. Aspecten: Tijdigheid, volledigheid, accuraatheid, consistentie, begrijpbaarheid, uniekheid Is er een strategie voor datakwaliteit?
	Nee: niveau 2 Ja: naar vraag 4
4.	Vindt er toetsing van de juistheid van persoonsgegevens (vergelijking met bron) plaats & worden er acties ondernomen bij het constateren van onjuistheid van gegevens?
	Nee: niveau 3 Ja: naar vraag 5
5.	Is er een strategie voor het verbeteren van de datakwaliteit?
	Nee: niveau 4 Ja: naar vraag 6

6.	Is sprake van benchmarking van de juistheid van gegevens en worden deze vergleken met andere organisaties?
	Nee: niveau 5 Ja: niveau 6
Score	

Rechtmatigheid, behoorlijkheid, transparantie

nummer	Vraag
1.	Is het eigenaarschap van gegevens binnen de organisatie vastgelegd?
	Nee: niveau 0 Ja: naar vraag 2
2.	Is er beleid vastgelegd voor m.b.t. tot het gebruik van persoonsgegevens en is dit beleid publieke toegankelijk?
	Nee: niveau 1 Ja: naar vraag 3
3.	Wordt er openlijk gecommuniceerd over het eigenaarschap en gebruik van persoonsgegevens?
	Nee: niveau 2 Ja: naar vraag 4
	Datagovernace: Data Governance is de uitoefening van autoriteit en controle (planning, monitoring en handhaving) op het beheren van 'data assets'
4.	Is datagovernace binnen de organisatie ingericht?
	Nee: niveau 3 Ja: naar vraag 5
5.	Zijn persoonsgegevens afgeschermd binnen de organisatie, zodat inzichtelijk is wie toegang heeft tot gegevens?
	Nee: niveau 4 Ja: naar vraag 6
6.	Kan de organisatie op korte termijn inzicht gegeven aan het gebruik van de persoonsgegevens van een eigenaar?
	Nee: niveau 4 Ja: naar vraag 6
7.	Is er een geautomatiseerd proces om toezicht te verkrijgen in het gebruik van persoonsgegevens
	Nee: niveau 5 Ja: niveau 6
Score	

Doelbinding

nummer	Vraag
1.	Is er een algemeen strekkende definitie van doelbinding binnen de organisatie en zijn medewerkers hiermee bekend?
	Nee: niveau 0 Ja: door naar vraag 2
2.	Is er een overkoepelend overzicht voor welke doelen de organisatie persoonsgegevens verzameld?
	Nee: niveau 1 Ja: door naar vraag 3
3.	Hoe wordt er invulling gegeven aan doelbinding binnen de datamanagementstrategie?
	Geen doelbinding in datamanagementstrategie: niveau 2 Ja. Vastleggen van doelbinding voor persoonsgegevens voor bepaalde datagroepen ingericht: niveau 3, naar vraag 4
4.	Worden persoonsgegevens binnen uw organisatie actief verwijderd als zij het verzameldoel hebben verloren en op basis van welke criteria gebeurt dit?
	Nee: niveau 3 Ja: geen duidelijke criteria, niveau 4 Ja: duidelijk criteria, niveau 5

5.	Op welke wijze wordt het borgen van doelbinding binnen de organisatie door ontwikkeld? (b.v. verplicht vast leggen van het verzameldoel)
	Verplichting vastlegging verzameldoel persoonsgegevens & toetsing verzameldoel: niveau 6 Geen vastlegging verzameldoel: niveau 5
Score	

Minimale gegevensverwerking

nummer	Vraag
1.	Welke definitie wordt er binnen de organisatie gehanteerd voor minimale gegevensverwerking?
	Geen definitie aanwezig: niveau 0 Informele of vastgestelde definitie: niveau 1, naar vraag 2
2.	Is er zicht op de verwerking van persoonsgegevens (worden deze nog actief gebruikt voor het doel waarvoor zij zijn verworven)?
	Er is geen inzicht in de verwerking: niveau 1 Er is per organisatieonderdeel inzicht in de verwerking : niveau 1, door naar vraag 3 Er is een organisatie breed inzicht in de verwerking van gegevens: niveau 2, door naar vraag 3
3.	Hoe is het toezicht op de rechtmatige verwerking van gegevens ingericht?
	Er is geen sprake van toezicht: niveau 1 of 2 (vraag 2) Er is sprake van centraal toezicht: niveau 3 of 4, door naar vraag 4
4.	Op welke wijze worden persoonsgegevens verwijderd nadat zij doelbindingen hebben verloren en hoe wordt dit gecontroleerd?
	Er is geen sprake van verwijdering/ vernietiging: niveau 3 of 4 Gegevens worden terstond vernietigd en er is sprake van centraal toezicht: niveau 5, door naar vraag 5
5.	Er wordt per verzameld veld gemotiveerd (b.v. naam/ geslacht) aangegeven waarom verzameling van dit gegeven dit noodzakelijk is.
	Sprake van motivering en vastlegging: niveau 6 Afwezig: niveau 5
Score	

Bijlage 16 Aangepaste scoringsvragen

Orginele vraag	**aangepaste vraag**
Wordt de opslag van persoonsgegevens op relevantie (is het doel waarvoor de gegevens zijn verworven nog steeds van toepassing) gecontroleerd?	Zijn de persoonsgegevens die worden verwerkt vastgesteld in een verwerkingsregister?
Zijn medewerkers zich bewust van deze standaarden?	Wordt de juistheid van persoonsgegevens bewaakt en is er de mogelijkheid persoonsgegevens te corrigeren?
Is er een bewuste strategie voor datakwaliteit?	Wordt de juistheid van persoonsgegevens organisatie breed op een eenduidige wijze bewaakt en formeel vastgesteld?
Vindt er toetsing van de juistheid van persoonsgegevens plaats (bv. door vergelijking met de informatiebron) en worden er acties ondernomen bij het constateren van onjuiste gegevens?	Is de juistheid van persoonsgegevens over de keten heen gegarandeerd?
Is er een strategie voor het verbeteren van de datakwaliteit?	Maakt de kwaliteit van persoonsgegevens integraal onderdeel uit van de management- en architectuurprocessen?
Is er sprake van benchmarking door de juistheid van gegevens te vergelijken met andere organisaties?	Stuurt het hoogste management op het bewaken van de juistheid van persoonsgegevens?
Is data governace binnen de organisatie ingericht?	Geschrapt
Welke definitie wordt er binnen de organisatie gehanteerd voor minimale gegevensverwerking?	Zijn de verplichte AVG rollen (zoals een FG) aanwezig binnen de organisatie & zien deze toe op minimale gegevensverwerking?
Hoe is het toezicht op de rechtmatige verwerking van gegevens ingericht?	Vindt het bepalen en omschrijven van de verzameldoeleinden en de rechtvaardigingsgronden organisatie breed op een eenduidige formele manier plaats?
Op welke wijze worden persoonsgegevens verwijderd nadat zij doelbindingen hebben verloren en hoe wordt dit gecontroleerd?	Worden de bepaalde en omgeschreven verzameldoeleinde en rechtvaardigingsgronden vergeleken met gelden gronden van vergelijkbare organisaties?

Bijlage 17 Aangepaste maturity levels juistheid

GDPR kernaspecten	0. afwezig	1.Initieel	2. basis	3. Managed	4. geoptimaliseerd	5. continu verbeterd
Juistheid (oude waarde)	Aandacht voor juistheid van persoonsgegevens is afwezig	Er is binnen de organisatie bewustzijn voor de juistheid van gegevens, er zijn standaarden voor datakwaliteit	Er is binnen de organisatie een begrip voor juistheid van gegevens. Er is een strategie voor datakwaliteit	De juistheid van persoonsgegevens wordt getoetst. Er wordt invulling gegevens aan de strategie voor datakwaliteit	De juistheid van gegevens getoetst en uit de uitkomsten wordt opvolging gegeven. Datakwaliteit wordt gemeten en hier wordt over gerapporteerd	Juistheid van gegevens wordt vergeleken met andere partijen, er is sprake van continue doorontwikkeling
Juistheid (nieuwe waarde)	Aandacht voor juistheid van persoonsgegevens is afwezig	Er is binnen de organisatie bewustzijn voor de juistheid van gegevens	Er is binnen de organisatie een begrip voor juistheid van gegevens	De juistheid van persoonsgegevens wordt getoetst.	De juistheid van gegevens getoetst en uit de uitkomsten wordt opvolging gegeven.	Juistheid van gegevens wordt vergeleken met andere partijen, er is sprake van continue doorontwikkeling

Bijlage 18 TAM vragenlijst

	Mate mee eens stelling			
Verwachte bruikbaarheid	Org 1, 1	Org 1, 2	Org 1, 3	Org 2
Ik geloof dat dit *maturity* model de inspanning zou verminderen die nodig is om de GDPR correct toe te passen.	6	2	3	5
Het documenteren van de GDPR implementatie door middel van dit *maturity* model zou lastig zijn om te begrijpen door gebruikers.	6	3	5	3
Met dit *maturity* model kunnen gebruikers gemakkelijker controleren of de GDPR correct wordt toegepast.	3	5	5	5
Over het algemeen vond ik het *maturity* model nuttig	5	5	5	5
Het gebruik van dit *maturity* model zou het moeilijker maken om de GDPR toe te passen.	6	3	6	2
Over het algemeen denk ik dat dit *maturity* model geen effectieve oplossing biedt voor het toepassen van de GDPR.	2	5	4	5
Over het algemeen denk ik dat dit *maturity* model een verbetering is voor de standaard implementatie van de GDPR.	6	5	5	5
Met behulp van dit *maturity* model zou het gemakkelijker zijn om GDPR implementatie naar de eindgebruiker te communiceren	5	6	2	6
verwachte gebruiksgemak	4,875	4,25	4,375	4,5
Ik vond de procedure voor het toepassen van het *maturity* model complex en moeilijk te volgen	6	5	6	6
Over het algemeen vond ik het *maturity* model moeilijk te gebruiken	6	6	6	6
Ik vond het *maturity* model eenvoudig om aan te leren	6	6	6	6
Ik vond het moeilijk om het *maturity* model toe te passen binnen mijn eigen bedrijfscontext	6	6	5	6
Ik vond de vragen van het *maturity* model duidelijk en gemakkelijk te begrijpen	4	3	6	6
Ik heb er geen vertrouwen in dat ik nu in staat ben om dit *maturity* smodel in de praktijk toe te passen	6	6	6	6
Intentie voor gebruik	5,666667	5,333333	5,833333	6
Ik zou dit *maturity* model zeker niet gebruiken om de GDPR correct toe te passen	6	6	6	6
Ik ben van plan om dit *maturity* model bij voorkeur te gebruiken voor toepassing van de GDPR in de toekomst	5	4	3	4
	5,5	5	4,5	5

Bijlage 19 Analyse van verschillende maturity levels

***Maturity* niveau**	**GOA 2.0**	**OMB 3.1**	**MD3M**	**DCAM**	**DMM**
0. afwezig	Creëren van EA awareness			Capabilities zijn ad-hoc en ongeorganiseerd	
1.Initieel	Creëren van EA instituties en commitment	1	Sprake van eerste bewustzijn	Eerste initiatieven zijn ontplooid en gepland	Processen zijn ad-hoc, reactief en worden niet toegepast over verschillende domeinen.
2. basic	Creëren van het managementfundament voor EA	2	Maatregelen van individuen worden uitgevoerd, geen verbinding met projecten.	Data initiatieven zijn gekoppeld aan organisatie doelstellingen	Processen worden gepland en uitgevoerd conform beleid door getrainde werknemers in samenspraak met relevante stakeholders
3. Managed	Initiële EA versies ontwikkelen	3	Eerste samenwerking op tactisch niveau. Bewustzijn wordt gecreëerd voor het bestaan van andere initiatieven.	Business gebruikers hebben een actieve rol in data management, DM prinses zijn gekoppeld aan organisatie doelstellingen	Een set van standaard processen is vastgelegd en wordt gevolgd. Specifieke behoeftes worden vervuld door processen conform beleid te baseren op de standaard processen,
4. geoptimaliseerd	Opleveren en gebruiken van EA om resultaten te leveren	4	Er zijn best practices voor het omgaan met MDM. Er zijn gedefinieerde processen op tactisch niveau	DM in geïncorporeerd in de bedrijfsvoering	Criteria voor processen zijn vastgelegd en worden gebruikt voor data management. Dit houdt in: management van afwijkingen, voorspellingen en analyse. Processen worden gemanaged tijdens de uitvoering.

	Door ontwikkelen van EA voor organisatie transformatie	5	Geoptimaliseer de gebruik MDM, de efficiëntie van de organisatie is verbeterd.	DM is geïncorporeer d in de bedrijfsvoering en organisatie cultuur	Processen worden geoptimaliseerd door het toepassen van niveau 4 analyse voor verbetermogelijkhed en. Best practices worden gedeeld met andere bedrijven.
5. continu verbeterd	Continu verbeteren van EA om organisatie optimalisatie te bereiken				

Bijlage 20 Scoring model vragen

	Org 1, 1	Org 1, 2	Org 1, 3	Org 2	interkwartielbereik <1,5	Consensus?	Kappa	Conclusie
Integriteit en vertrouwelijkheid								
1. Is er binnen de organisatie aandacht voor de Integriteit en vertrouwelijkheid van persoonsgegevens?	6	6	6	7	0,50	Ja	NVT	Behouden
2. Zijn er binnen uw organisatie standaarden gericht op integriteit en vertrouwelijkheid voor implementatie van nieuwe dataoplossingen, en zo ja welke zijn dit?	6	6	6	6	0,00	Ja	NVT	Behouden
3. Wordt er logging toegepast bij het raadplegen of muteren van gegevens binnen de organisatie?	6	7	6	6	0,50	Ja	NVT	Behouden
4. Wordt de toegang tot persoonsgegevens op basis van rollen verstrekt	6	7	6	7	1,00	Ja	NVT	Behouden
5. Zijn medewerkers zich bewust van informatiebeveiliging? En welke voor maatregelen zijn er door de organisatie genomen om dit bewustzijn te borgen?	6	6	6	6	0,00	Ja	NVT	Behouden
6. Hoe wordt er door de organisatie geleerd op het gebied van informatiebeveiliging en hoe wordt deze informatie gedeeld?	6	6	4	6	1,00	Ja	NVT	Behouden
Opslagbeperking								
1. Zijn er beperkingen binnen de organisatie voor de opslag van persoonsgegevens?	6	7	6	6	0,50	Ja	NVT	Behouden
2. Is datalifecycle management ingericht, wordt er actief onderscheid gemaakt tussen de verschillende fases in de levenscyclus?	6	5	5	6	1,00	Ja	NVT	Behouden

3. Welke datadomeinen worden er onderscheiden binnen de organisatie?	6	6	4	6	1,00	Ja	NVT	Behouden
4. Wordt de opslag van persoonsgegevens op relevantie (is het doel waarvoor de gegevens zijn verworven nog steeds van toepassing) gecontroleerd?	6	4	5	7	2,00	Nee	0,25	Aanpassen
5. Is er sprake van enkelvoudige opslag (ipv opslag per toepassing/applicatie) van gegevens?	6	5	5	7	1,50	Ja	NVT	Behouden
6. Is er een vaststaand proces waarbij rollen en mutaties rechten zijn vastgelegd voor het wijzigingen van persoonsgegevens ingericht?	6	6	6	6	0,00	Ja	NVT	Behouden
Juistheid								
1. Zijn er standaarden of eisen voor de juistheid van gegevens binnen uw organisatie?	6	6	5	6	0,50	Ja	NVT	Behouden
2. Zijn medewerkers zich bewust van deze standaarden?	6	5	4	6	1,50	Ja	NVT	Behouden
3. Is er een bewuste strategie voor datakwaliteit?	6	6	3	6	1,50	Ja	NVT	Behouden
4. Vindt er toetsing van de juistheid van persoonsgegevens plaats (bv. door vergelijking met de informatiebron) en worden er acties ondernomen bij het constateren van onjuiste gegevens?	6	6	3	6	1,50	Ja	NVT	Behouden
5. Is er een strategie voor het verbeteren van de datakwaliteit?	6	6	3	6	1,50	Ja	NVT	Behouden
6. Is er sprake van benchmarking door de juistheid van gegevens te vergelijken met	5	4	2	4	1,50	Nee	-0,25	Aanpassen

andere organisaties?								
Rechtmatigheid, behoorlijkheid, transparantie								
1. Is het eigenaarschap van gegevens binnen de organisatie vastgelegd?	6	7	6	6	0,50	Ja	NVT	Behouden
2. Is er beleid vastgelegd voor het gebruik van persoonsgegevens en is dit beleid publiek toegankelijk?	6	7	6	6	0,50	Ja	NVT	Behouden
3. Wordt er openlijk gecommuniceerd over het eigenaarschap en het gebruik van persoonsgegevens?	6	7	6	6	0,50	Ja		Behouden
4. Is data governace binnen de organisatie ingericht?	6	3	6	6	1,50	Ja	NVT	Behouden
5. Zijn persoonsgegevens afgeschermd binnen de organisatie, zodat inzichtelijk is wie toegang heeft tot gegevens?	6	6	6	6	0,00	Ja	NVT	Behouden
6. Kan de organisatie op korte termijn inzicht gegeven aan het gebruik van de persoonsgegevens van een eigenaar?	6	6	6	6	0,00	Ja	NVT	Behouden
7. Is er een geautomatiseerd proces om toezicht te verkrijgen in het gebruik van persoonsgegevens?	6	6	4	6	1,00	Ja	NVT	Behouden
Doelbinding								
1. Is er een algemeen strekkende definitie van doelbinding binnen de organisatie en zijn medewerkers hiermee bekend?	5	5	6	6	1,00	Ja	NVT	Behouden
2. Is er een overkoepelend overzicht voor welke doelen de organisatie persoonsgegevens verzameld?	5	7	6	6	1,00	Ja	NVT	Behouden
3. Hoe wordt er invulling gegeven aan	5	5	4	6	1,00	Ja	NVT	Behouden

doelbinding binnen de datamanagementstrategie?								
4. Worden persoonsgegevens binnen uw organisatie actief verwijderd als zij het verzameldoel hebben verloren en op basis van welke criteria gebeurt dit?	6	4	6	6	1,00	Ja	NVT	Behouden
5. Op welke wijze wordt de doelbinding van gegevens binnen de organisatie gegarandeerd en getoetst? (b.v. verplicht vast leggen van het verzameldoel)	6	6	4	6	1,00	Ja	NVT	Behouden
Minimale gegevensverwerking								
1. Welke definitie wordt er binnen de organisatie gehanteerd voor minimale gegevensverwerking?	5	7	4	6	2,00	Nee	0,25	Aanpassen
2. Is er zicht op de verwerking van persoonsgegevens binnen de organisatie (bv. worden deze nog actief gebruikt voor het doel waarvoor zij zijn verworven)?	6	5	6	6	0,50	Ja	NVT	Behouden
3. Hoe is het toezicht op de rechtmatige verwerking van gegevens ingericht?	6	5	4	6	1,50	Ja	NVT	Behouden
4. Op welke wijze worden persoonsgegevens verwijderd nadat zij doelbindingen hebben verloren en hoe wordt dit gecontroleerd?	6	5	4	6	1,50	Ja	NVT	Behouden
5. Er wordt per verzameld veld gemotiveerd (b.v. naam/ geslacht) aangegeven waarom verzameling van dit gegeven dit noodzakelijk is?	6	7	6	6	0,50	Ja	NVT	Behouden

Bijlage 21 Scoring aangepaste model vragen

Aangepaste vraag	Org 1, 1	Org 1, 2	Org 2	interkwartielbereik <1,5	Consensus?	Kappa	Conclusie
Zijn de persoonsgegevens die worden verwerkt vastgesteld in een verwerkingsregister?	6	5	7	2	Nee	1.00	Behouden
Wordt de juistheid van persoonsgegevens bewaakt en is er de mogelijkheid persoonsgegevens te corrigeren?	6	5	7	2	Nee	1.00	Behouden
Wordt de juistheid van persoonsgegevens organisatie breed op een eenduidige wijze bewaakt en formeel vastgesteld?	7	6	7	1	ja	NVT	Behouden
Is de juistheid van persoonsgegevens over de keten heen gegarandeerd?	5	5	6	1	ja	NVT	Behouden
Maakt de kwaliteit van persoonsgegevens integraal onderdeel uit van de management- en architectuurprocessen?	6	6	6	0	ja	NVT	Behouden
Stuurt het hoogste management op het bewaken van de juistheid van persoonsgegevens?	5	5	7	2	Nee	1.00	Behouden
Zijn de verplichte AVG rollen (zoals een FG) aanwezig binnen de organisatie & zien deze toe op minimale gegevensverwerking?	7	6	6	1	ja	NVT	Behouden
Vindt het bepalen en omschrijven van de verzameldoeleinden en de rechtvaardigingsgronden organisatie breed op een eenduidige formele manier plaats?	6	5	7	2	Nee	1.00	Behouden

Worden de bepaalde en omgeschreven verzameldoeleinde en rechtvaardigingsgronden vergeleken met gelden gronden van vergelijkbare organisaties?	6	2	4	4	Nee	-0,5	Schrappen

Bijlage 22 Algemene tevredenheidsscore

Ronde 1	
Org 1, 1	9
Org 1, 2	5
Org 1, 3	6
Org 2	8
gemiddeld	7
Ronde 2	
Org 1, 1	7
Org 1, 2	8
Org 1, 3	6
Org 2	9
gemiddeld	7,5

Bijlage 23 Aangepast GDPR *maturity model*

GDPR kernaspecten	**0. afwezig**	**1.Initieel**	**2. basis**	**3.Managed**	**4. geoptimaliseerd**	**5. continu verbeterd**
Integriteit en vertrouwelijkheid	Aandacht voor integriteit en vertrouwelijkheid van persoonsgegevens is afwezig	Aan technische eisen de beveiliging van persoonsgegevens is voldaan. Nieuwe oplossingen die persoonsgegevens verwerken worden getoetst aan deze standaarden	Er wordt gelogd wie toegang heeft tot persoonsgegevens, er is een datamanagement strategie	Toegang tot persoonsgegevens wordt op basis van rules verstrekt. Er is aandacht voor rationalisatie van persoonsgegevens	Beveiligingsbeleid berust op standaarden, er een datamanagement strategie, Er is bewustzijn onder medewerkers voor informatiebeveiliging	Informatiebeveiliging wordt continu door ontwikkeld en verbeterd
Opslagbeperking	Aandacht voor opslagbeperking van persoonsgegevens is afwezig	Data is logisch opgeslagen, de organisatie is bekend met data lifecycle management	Opgeslagen persoonsgegevens worden gecontroleerd. Data is logisch opgedeeld in domeinen.	Er is regelmatig controle op de noodzaak van het opslaan van persoonsgegevens.	Er is sprake van één singel source of truth voor persoonsgegeven. Persoonsgegevens worden enkelvoudig opgeslagen.	Persoonsgegevens zijn op innovatieve wijze opgeslagen, er is logging op door wie deze gegevens worden geraadpleegd.
Juistheid	Aandacht voor juistheid van persoonsgegevens is afwezig	Er is binnen de organisatie bewustzijn voor de juistheid van gegevens	Er is binnen de organisatie een begrip voor juistheid van gegevens	De juistheid van persoonsgegevens wordt getoetst.	De juistheid van gegevens getoetst en uit de uitkomsten wordt opvolging gegeven.	Juistheid van gegevens wordt vergeleken met andere partijen, er is sprake van continue doorontwikkeling

GDPR kernaspecten	0. afwezig	1.Initieel	2. basis	3.Managed	4. geoptimaliseerd	5. continu verbeterd
rechtmatigheid, behoorlijkheid, transparantie	Aandacht voor rechtmatigheid, behoorlijkheid, transparantie is afwezig	Eigenaarschap voor gegevens is vastgelegd, er is zicht op wie welke gegevens gebruikt	Eigenaarschap voor gegevens is vastgelegd, en dit wordt gecommuniceerd. Er is sprake van data governance.	Data governance is organisatie breed ingericht, persoonsgegevens zijn alleen toegankelijk wanneer strikt noodzakelijk	Er is zicht op al het datagebruik binnen de organisatie, dit gebruik wordt gecommuniceerd	Data governance is organisatie breed ingericht en wordt continu verbeterd
Doelbinding	Aandacht voor doelbinding is afwezig	Er is een basis definitie voor doelbinding binnen de organisatie	Er is een data management strategie waar doelbinding wordt geadresseerd	Inzicht voor welke doelen persoonsgegevens over de organisatie heen worden verzameld en welke doel aan welke data is gekoppeld	Persoonsgegevens die niet aan een doel te koppelen zijn worden actief verwijderd.	Doelbinding van persoonsgegevens wordt continu doorontwikkeld
Minimale gegevensverwerking	Aandacht voor minimale gegevensverwerking is afwezig	Er is een definitie voor minimale gegevensverwerking	Er is bekend wie welke gegeven binnen een organisatie kunnen verwerken	Er is bekend of persoonsgegevens (rechtmatig) worden gebruikt	Persoonsgegevens die niet worden gebruikt worden verwijderd	Minimale gegevensverwerking wordt continu doorontwikkeld